Microsoft

Configuring Windows® 8

Training Guide

Scott D. Lowe
Derek Schauland
Rick W. Vanover

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

Copyright © 2013 by Scott Lowe

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2012955627
ISBN: 978-0-7356-7322-9

Printed and bound in the United States of America.

First Printing

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

Microsoft and the trademarks listed at http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx are trademarks of the Microsoft group of companies. All other marks are property of their respective owners."

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Project Editor: Karen Szall
Editorial Production: nSight, Inc.
Technical Reviewer: Michael Toot; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Kerin Forsyth
Indexer: Lucie Haskins
Cover: Microsoft Press Brand Team

Contents at a glance

Introduction *xix*

CHAPTER 1 Evaluating Windows 8 1

CHAPTER 2 Installing and migrating to Windows 8 37

CHAPTER 3 Handling hardware and device drivers 79

CHAPTER 4 Installing and configuring applications 119

CHAPTER 5 Managing Internet Explorer 145

CHAPTER 6 Using Hyper-V 181

CHAPTER 7 Administering Windows networking 223

CHAPTER 8 Configuring security 261

CHAPTER 9 Working with remote management tools 293

CHAPTER 10 Sharing resources 343

CHAPTER 11 File system and storage management 371

CHAPTER 12 Administering authentication and authorization 419

CHAPTER 13 Managing and securing mobility 463

CHAPTER 14 Monitoring and maintaining Windows 487

CHAPTER 15 System protection and recovery 527

Index *559*

Contents

Introduction **xix**

System requirements *xix*

Practice setup instructions *xxi*

Acknowledgments *xxi*

Errata & book support *xxii*

We want to hear from you *xxii*

Stay in touch *xxii*

Chapter 1 Evaluating Windows 8 **1**

Lesson 1: What’s new in Windows 8 1

Navigating the Windows 8 user interface 2

Introducing some new features 12

Lesson summary 24

Lesson review 24

Lesson 2: Understanding product editions, architectures, and hardware requirements 25

Windows 8 product edition differences 26

Windows 8 product architecture differences 28

Windows 8 hardware requirements 29

Lesson summary 31

Lesson review 31

Practice exercises 32

Exercise 1: Add an Internet Explorer shortcut to the Start screen 32

Exercise 2: Configure user settings to synchronize between Windows 8 devices 33

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:

www.microsoft.com/learning/booksurvey/

Suggested practice exercises 33

Answers. 34

Chapter 2 Installing and migrating to Windows 8 37

Lesson 1: Installing Windows 8 on a new or formatted system 38

Starting the installation 38

Configuring your account 40

Joining an Active Directory domain 44

Installing Windows 8 with Windows To Go 44

Lesson summary 48

Lesson review 49

Lesson 2: Upgrading or migrating from a previous version of Windows. 49

Running the Setup Wizard 50

Configuring your account 51

Upgrading from Windows Vista 52

Upgrading from Windows XP 52

Moving and transferring files by using Windows Easy Transfer 52

Lesson summary 64

Lesson review 64

Lesson 3: Installing Windows 8 on startup VHD files 65

Creating a VHD from an existing installation 66

Creating the VHD during the installation by using DiskPart 68

Starting the system from the VHD 69

Removing VHD installations 71

Lesson summary 72

Lesson review 72

Practice exercises 73

Exercise 1: Install Windows 8 73

Exercise 2: Configure Windows 8 to start from a VHD 74

Exercise 3: Set up a Windows To Go workspace 74

Suggested practice exercises 75

Answers. 76

Chapter 3 Handling hardware and device drivers 79

Lesson 1: Managing drivers. 79

Driver installation methods 80

Driver types 81

Using Device Manager 81

Using the System Information utility 93

Discovering the Driver Verifier utility 95

Adding device drivers to the driver store 102

Lesson summary 103

Lesson review 103

Lesson 2: Managing hardware devices 104

Enabling and disabling hardware devices 104

Monitoring USB devices 105

Lesson summary 107

Lesson review 107

Lesson 3: Managing enterprise hardware policies 107

Managing enterprise hardware installation policies 108

Lesson summary 113

Lesson review 114

Practice exercises 114

Exercise 1: Locate hardware ID for a USB thumb drive 114

Exercise 2: Create Group Policy to prevent the installation of hardware devices 115

Suggested practice exercises 115

Answers. 116

Chapter 4 Installing and configuring applications 119

Lesson 1: Managing traditional desktop applications 119

Using Windows Installer in Windows 8 120

Running Windows Installer packages and MSIExec 120

Managing compatibility with Application Compatibility Toolkit and App-V 122

Controlling program settings for traditional applications 123

Lesson summary 126

Lesson review 127

Lesson 2: Managing Windows 8 native applications 128

Installing, updating, and uninstalling Windows 8 native applications 128

Reinstalling apps that have been removed 129

Acquiring desktop apps in the Windows Store 131

Disabling and controlling access to the Windows Store app 131

Managing access to hardware and installed applications 132

Controlling applications by using AppLocker 133

Sideloading apps in Windows 8 137

Inventorying and removing apps 139

Lesson summary 140

Lesson review 140

Practice exercises 141

Exercise 1: Install line-of-business applications 142

Exercise 2: Prevent access to the Windows Store 142

Suggested practice exercises 142

Answers. 143

Chapter 5 Managing Internet Explorer 145

Lesson 1: Configuring Internet Explorer 10 145

Managing two Internet Explorer experiences 146

Managing Internet Explorer settings by using Group Policy 153

Lesson summary 155

Lesson review 155

Lesson 2: Understanding and configuring browser security settings . . .156

Managing new Internet Explorer 10 security settings 156

Adding trusted sites to Internet Explorer 162

Managing Internet Explorer security settings by using Group Policy 162

Lesson summary 164

Lesson review 164

Lesson 3: Managing Internet Explorer add-ons 165

Understanding add-ons 165

Managing ActiveX controls 166

Managing other add-ons 169

Managing Internet Explorer add-ons by using Group Policy 172

Lesson summary 175

Lesson review 176

Practice exercises 176

Exercise 1: Configure ActiveX (Internet zone) 176

Exercise 2: Disable the Map With Bing accelerator 177

Suggested practice exercises 177

Answers. 178

Chapter 6 Using Hyper-V 181

Lesson 1: Learning about Hyper-V for Windows 8 181

Introducing Hyper-V for Windows 8 182

When to use Hyper-V 183

Data management and licensing 184

Enabling Hyper-V 185

What you need to know to succeed 186

Lesson summary 190

Lesson review 191

Lesson 2: Creating and using Hyper-V virtual machines 191

Planning your virtual machines 192

Creating a new virtual machine 195

Using a Hyper-V virtual machine 202

Lesson summary 206

Lesson review 207

Lesson 3: Configuring virtual machine networking and storage 208

Introducing storage and networking for Hyper-V 208

Hyper-V virtual switch 210

Lesson summary 216

Lesson review 217

Practice exercises 217

Exercise 1: Create a virtual machine 217

Exercise 2: Customize a virtual machine 218

Suggested practice exercises 218

Answers. 219

Chapter 7 Administering Windows networking 223

Lesson 1: Configuring networking 223

What’s new in networking in Windows 8 224

Installing a network adapter 227

Managing network settings 228

Connecting to a wireless network 241

Lesson summary 246

Lesson review 246

Lesson 2: Troubleshooting networking 247

Updating the Task Manager view for networking 247

Viewing Windows 8 network settings 249

Using the network troubleshooters 252

Using command-line tools 254

Lesson summary 255

Lesson review 255

Practice exercises 256

Exercise 1: Disable Network Discovery on the Private network profile 256

Exercise 2: Manually configure IP settings for one of your network adapters 256

Exercise 3: Use the netstat command 257

Suggested practice exercises 257

Answers. 258

Chapter 8 Configuring security 261

Lesson 1: Managing Windows Firewall and exceptions 261

Choosing Windows Firewall 262

Choosing Windows Firewall with Advanced Security 264

Monitoring rules configured in Windows Firewall 274
Lesson summary 274
Lesson review 275

Lesson 2: Configuring network discovery and wireless security. 275
Creating network discovery profiles 276
Managing wireless security 280
Understanding types of wireless security 281
Wireless networking risks 282
Reducing security issues on a wireless network 282
Lesson summary 283
Lesson review 283

Lesson 3: Using Secure Boot and SmartScreen Filter 284
Ensuring that Windows has been signed using Secure Boot 284
Staying safe by using SmartScreen Filter 285
Lesson summary 286
Lesson review 287

Practice exercises 287
Exercise 1: Configure inbound firewall rules for programs 287
Exercise 2: Configure outbound firewall rules for ports 288
Exercise 3: Configure firewall exceptions 288

Suggested practice exercises 289

Answers. 290

Chapter 9 Working with remote management tools 293

Lesson 1: Working with Remote Assistance 294
Initiating Remote Assistance 294
Providing remote assistance 296
Lesson summary 297
Lesson review 298

Lesson 2: Configuring and using Remote Desktop. 298
Configuring Remote Desktop 299
Opening the Remote Desktop application 301
Lesson summary 308
Lesson review 308

Lesson 3: Configuring, managing, and troubleshooting connections . . 309
Troubleshooting network problems 310
Using Troubleshooter 313
Connecting to VPNs in Windows 8 315
Lesson summary 322
Lesson review 322

Lesson 4: Using other management tools remotely 323
Netsh 324
Windows Remote Shell 325
Windows PowerShell 326
Microsoft Management Console 328
Lesson summary 334
Lesson review 334

Practice exercises 335
Exercise 1: Configure a Remote Desktop session that launches PowerShell.exe and connect to a remote computer 335
Exercise 2: Help another user initiate a Remote Assistance session 336
Exercise 3: Work with Windows PowerShell to obtain information about a remote system 336

Suggested practice exercises 337

Answers. 338

Chapter 10 Sharing resources 343

Lesson 1: Sharing files and folders. 343
Configuring the Network and Sharing Center 344
Sharing files and folders 346
Understanding NTFS permissions 352
Lesson summary 363
Lesson review 363

Lesson 2: Sharing printers 364
Configuring shared printers 364
Configuring printing permissions 366
Lesson summary 367
Lesson review 367

Practice exercises 368

Exercise 1: Enable file sharing for a network adapter in your lab server 368

Exercise 2: Test each other 368

Suggested practice exercises 368

Answers. 369

Chapter 11 File system and storage management 371

Lesson 1: Managing disks and storage 371

Using disk management 372

Disk Defragmenter and Disk Cleanup 377

Using Microsoft Drive Optimizer to organize data 380

Lesson summary 390

Lesson review 390

Lesson 2: Working with file systems 391

Security within the file system 391

Inheritance and cumulative effectiveness 397

Taking ownership 399

Understanding share-level permissions 400

Auditing access to securable objects by using SACLs 400

Understanding Encrypting File System 402

BitLocker 404

Working with quotas 405

Working with quotas for user accounts 407

Lesson summary 408

Lesson review 408

Lesson 3: Introducing Storage Spaces 409

What is Storage Spaces? 409

Creating storage spaces 410

Lesson summary 413

Lesson review 413

Practice exercises 414

Exercise 1: Use disk optimizer 414

Exercise 2: Configure Storage Spaces 415

Suggested practice exercises 415

Answers. 416

Chapter 12 Administering authentication and authorization 419

Lesson 1: Determining who's who through authentication. 419

What is authentication and what does it do? 420

How does Windows authenticate users accessing the system? 420

User name and password-based authentication 422

Smart card authentication 425

Biometric authentication 427

Managing credentials in Windows 8 by using Credential Manager 428

Configuring a Microsoft account for use with Windows 430

Logging on by using a picture password 432

Using a personal identification number (PIN) for authentication 435

Lesson summary 436

Lesson review 436

Lesson 2: Managing authorization and access rights. 437

Getting started with user rights 437

Working in groups 438

Understanding rights vs. permissions 438

Assigning user rights 438

Local Security Policy console 443

Running tasks as administrator and user account control 452

Run As 454

Using and managing certificates 455

Lesson summary 458

Lesson review 458

Practice exercises 459

Exercise 1: Configure a Microsoft account for authentication 459

Exercise 2: Configure a picture password and PIN for sign-in 459

Exercise 3: Run applications with elevated privileges 460

Suggested practice exercises 460

Answers. 461

Chapter 13 Managing and securing mobility 463

Lesson 1: Managing BitLocker and other policy-based mobility tools . 463

Configuring BitLocker policies 464

Managing BitLocker at the command line 466

Using BitLocker on computers without TPM 468

Using BitLocker on removable media (BitLocker To Go) 470

Configuring policy settings for offline files 471

Configuring offline file synchronization 473

Configuring policy settings for device power 476

Lesson summary 478

Lesson review 478

Lesson 2: Working with location-based settings and connection methods 480

Connecting to devices by using Wi-Fi Direct 480

Using airplane mode and location-based services in Windows 8 481

Lesson summary 482

Lesson review 482

Practice exercises 483

Exercise 1: Configure BitLocker and BitLocker To Go 483

Exercise 2: Configure subfolder availability for offline files 483

Exercise 3: Configure actions for the power button 483

Suggested practice exercises 484

Answers. 485

Chapter 14 Monitoring and maintaining Windows 487

Lesson 1: Managing Windows Update 487

Accessing Windows Update settings by using Control Panel 488

Configuring update settings 490

Identifying new updates 493

Managing Windows Update in Windows 8 native interface 494

Viewing update history 496

Rolling back updates 497

Configuring Windows Update policies 499

Lesson summary 500
Lesson review 500

Lesson 2: Monitoring, optimizing, and troubleshooting system health and performance. 501
Managing and monitoring the system by using Task Manager 502
Using Windows Action Center 511
Configuring and analyzing event logs 513
Monitoring system resources by using Performance Monitor 517
Lesson summary 521
Lesson review 522

Practice exercises 522
Exercise 1: Enable automatic updates on your computer 522
Exercise 2: Manually end a process in Windows 523
Exercise 3: Create an event log filter 523

Suggested practice exercises 523

Answers. 524

Chapter 15 System protection and recovery 527

Lesson 1: Working with backup and restoration. .528
Backing up Windows 8 528
Creating additional images 530
Protecting files and data by using File History 530
Restoring an entire computer 535
Using System Restore for less invasive troubleshooting 536
Two new methods of restoration and recovery 539
Lesson summary 543
Lesson review 543

Lesson 2: Advanced settings and features for Windows recovery 544
MSConfig 544
Task Manager Startup 546
Recovering from a bad driver installation 546
Lesson summary 547
Lesson review 547

Lesson 3: Advanced recovery and restoration options 548

Creating a system repair or recovery disc 549
Using Windows Recovery Environment 550
Lesson summary 552
Lesson review 552

Practice exercises 553
Exercise 1: Back up files in Windows 8 553
Exercise 2: Recover files by using File History 553
Exercise 3: Bring your computer back to new with a reset 554
Exercise 4: Use Advanced Startup to troubleshoot problems with Windows 8 554

Suggested practice exercises 554

Answers. 555

Index *559*

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:

www.microsoft.com/learning/booksurvey/

Introduction

This training guide is designed for information technology (IT) professionals who support or plan to support Windows 8 and are ramping up on the latest technology. It is assumed that before you begin using this guide, you have at least an entry-level understanding of Microsoft Windows and common Internet technologies.

This book covers some of the topics and skills that are the subject of the Microsoft certification 70-687 exam. If you are using this book to complement your study materials, you might find this information useful. This book is designed to help you in the job role; it might not cover all exam topics. If you are preparing for the exam, you should use additional study materials to bolster your real-world experience. For your reference, a mapping of the topics in this book to the exam objectives is included in the back of the book.

By using this training guide, you will learn how to do the following:

- Install Windows 8 on a new computer or upgrade to Windows 8 from an earlier version of Windows
- Share network resources, including printers and file storage space on a Windows 8 client
- Navigate the new Windows 8 user interface and perform common administrative tasks in both the new and the earlier interfaces
- Manage the Windows 8 client-side Hyper-V virtualization software
- Configure and manage Internet Explorer 10
- Manage and troubleshoot hardware device drivers
- Secure the Windows 8 operating system environment

System requirements

The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. To minimize the time and expense of configuring physical computers for this training guide, it's recommended that you use Hyper-V, which is a feature of Windows Server 2008, Windows Server 2008 R2, Windows 8, and Windows Server 2012. You can use other virtualization software instead, such as Windows Virtual PC or VirtualBox. If you do not have a way to create a virtual environment, have two physical PCs capable of running Windows 8 so that you can take full advantage of the training in this guide.

NOTE **REQUIREMENTS FOR A FULL TEST OF HYPER-V**

If you want to test the Hyper-V feature in Windows 8 fully, you must use a physical computer that supports Second Level Address Translation or a visualization platform that allows other virtualization platforms to run inside it. Such platforms include VMware Workstation 8 or higher and VMware Fusion 4 or higher.

Hardware requirements

This section presents the hardware requirements for Hyper-V, the hardware requirements if you are not using virtualization software, and the software requirements.

Virtualization hardware requirements

If you choose to use virtualization software, you need only one physical computer to perform the exercises in this book. That physical host computer must meet the following minimum hardware requirements:

- x64-based processor that includes both hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection. (On AMD systems, the data execution protection feature is called the No Execute or NX bit. On Intel systems, this feature is called the Execute Disable or XD bit.) These features must also be enabled in the BIOS. (You can run Windows Virtual PC without Intel-VT or AMD-V.)
- 4.0 GB of RAM (more is recommended)
- 120 GB of available hard disk space
- DVD-ROM drive
- Internet connectivity

Physical hardware requirements

If you choose to use physical computers instead of virtualization software, use the following list to meet the minimum hardware requirements of the practice exercises in this book:

- Three personal computers, each with a 1-GHz processor, 512 MB of RAM, network card, video card, and DVD-ROM drive
- At least 25 GB of disk space available on each computer
- All three computers physically connected to each other and to the Internet

Software requirements

The following software is required to complete the practice exercises:

- Windows 8. You can download an evaluation edition of Windows 8 at *http://technet.microsoft.com/en-us/windows/windows-8.aspx*.
- The Windows Assessment and Deployment Kit (Windows ADK) for Windows 8. You can find an overview of Windows ADK at *http://technet.microsoft.com/en-us/library/hh824947.aspx*, and the download is available at *http://www.microsoft.com/en-us/download/details.aspx?id=30652*.
- A web browser such as Internet Explorer 8 or later.

Practice setup instructions

Most of the practice exercises in this training guide require only a single computer, but for full testing, a second computer is often useful. For example, after you learn how to create a file share, you can then test your work by browsing to that file share from the other computer.

Acknowledgments

The authors would like to thank a number of people who helped in the creation of this Training Guide.

SCOTT LOWE

As is the case with everything I do, I dedicate this work to my beautiful wife, Amy, and my life-enriching, wonderful children, Ryan and Isabella. Without you, none of this would matter.

I also thank my coauthors, Derek Schauland and Rick Vanover, for their tireless efforts in getting this work to print.

DEREK SCHAULAND

This project has been one of the largest single writing projects that I have taken on, and although it was quite a bit of work to get to this point, we got it done. I have a newfound understanding of the work that goes into the certification process; for me, no longer is it about exams as much as it is about the entire process, from learning content all the way to the test.

I thank my wife Laura for encouraging me to keep going even when activities were popping up all the time. I also thank my friends and other family members for continuing to show interest in how the writing was going. It amazes me how much this helps the focus stick.

Last but certainly not least, I thank my fellow authors, Scott Lowe and Rick Vanover. Without the two of you, this project wouldn't have crossed my radar.

Thank you for the amazing opportunity.

RICK VANOVER

Rick dedicates his work in this book to his wife Amie and daughter Rilee.

Errata & 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 on our Microsoft Press site:

http://www.microsoftpressstore.com/title/9780735673229

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 mspinput@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 our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

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

Stay in touch

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

CHAPTER 3

Handling hardware and device drivers

Hardware and software are linked. Windows 8 is an operating system that unlocks the power of hardware; it's the hardware that people manipulate to do their work. This chapter discusses the components that enable hardware devices in Windows 8.

Some of the lessons in this chapter assume that, as an enterprise IT pro, you are already familiar with how to use Group Policy. This book does not go into detail about how to create Group Policy, but it does provide guidance on how administrators can use individual Group Policy settings to accomplish goals across the organization.

Lessons in this chapter:

- Lesson 1: Managing drivers **79**
- Lesson 2: Managing hardware devices **104**
- Lesson 3: Managing enterprise hardware policies **107**

Before you begin

To complete the practice exercises in this chapter, you will need:

- A USB device

Lesson 1: Managing drivers

Drivers are the software components that enable hardware to work in Microsoft Windows; device drivers enable communication between the operating system and hardware devices.

Remember these facts as you work with device drivers:

- Drivers are just software components.
- Not all drivers are created equal.
- Driver issues can be a support difficulty.
- Poorly written drivers can create system instability.

As an IT administrator in the enterprise, you will have to deal with installing hardware, updating driver software, and troubleshooting driver-related hardware issues.

After this lesson, you will be able to:

- Effectively use Device Manager to troubleshoot driver issues.
- Understand the purpose of the Driver Verifier utility and how to use it.
- Gather information from System Information to aid in troubleshooting.
- Update driver software to enable new features and close security holes.

Estimated lesson time: 60 minutes

Driver installation methods

Drivers can be added to a Windows system in a number of ways. The most common method is through the installation of Windows 8. During installation, drivers are installed for all the devices that are present.

- **Windows Update** In some cases, new drivers are installed or updated through regular Windows updates. As new drivers become available—particularly from Microsoft—they are delivered through the Windows Update process.
- **Hardware installation disc** Many devices ship with a hardware installation CD that includes all the drivers and software necessary to enable the device to operate. Just place the installation media into the CD-ROM drive of the computer and follow the installation instructions that came with the device.

  In some cases, device installation instructions require you to run the installation CD before you install the hardware so that the drivers are ready when the device is ultimately installed.
- **Internet download** As the age of the optical drive comes to an end, most companies also make driver and software downloads, which replace the antiquated CD, available on their websites. However, downloads are just new media for a new century. Otherwise, the installation process is the same as it is when using an installation disc.
- **Pre-staging drivers** In many organizations, administrators pre-stage drivers by installing all the drivers that someone might need before deploying a new computer. You learn more about pre-staging drivers in this chapter in the “Adding device drivers to the Driver Store” section.

Driver types

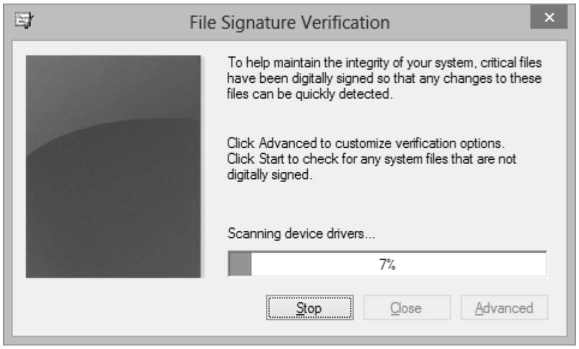
Two kinds of drivers are available: signed and unsigned. A signed driver carries with it a digital signature that verifies the publisher of the driver and ensures that the driver file has not undergone unauthorized modification, so it is less likely that someone has added malicious code to the driver file that could compromise the security of the system.

> ***IMPORTANT*** **DRIVER SIGNING IS NOT A CURE-ALL**
>
> **Although driver signing improves the overall security of the system, it's important to remember that driver signing alone will not fix every security issue. It's still possible for bad code to be introduced in a driver before the signing process or for an unauthorized entity to attain access to driver signing. Either way, use caution, even with signed drivers.**

An unsigned driver does not carry any guarantee that the company that issued it is legitimate, and there is no guarantee that the driver file has not been tampered with. Unsigned drivers are more likely to carry a driver file containing malware or be untrustworthy.

Remember that user-mode device drivers operate at a high level in the operating system with user rights. Kernel-mode drivers can create a major security issue.

You can use the Sigverif.exe utility to determine whether the files and drivers on a computer have been signed. To use Sigverif.exe, type **sigverif.exe** at a command prompt to open the Signature Verifier utility. Click Start to begin the scanning process. The utility displays the scanning progress, as shown in Figure 3-1.


File Signature Verification

To help maintain the integrity of your system, critical files have been digitally signed so that any changes to these files can be quickly detected.

Click Advanced to customize verification options.
Click Start to check for any system files that are not digitally signed.

Scanning device drivers...

FIGURE 3-1 The File Signature Verification process

Using Device Manager

In Windows 8, Device Manager is the utility that manages driver software, which includes updating and configuring drivers. If you've used Device Manager in previous versions of Windows, you will already be familiar with Device Manager as it appears in Windows 8. If you're new to managing hardware and drivers in Windows, this section introduces you to Device Manager.

IMPORTANT **WINDOWS 8 AND WINDOWS RT ARE MANAGED DIFFERENTLY**

This chapter discusses managing a full Windows 8 installation on x86 hardware. Devices that use Windows RT are not managed by using the techniques described here. Instead, those devices are managed by using an upcoming version of Windows InTune or by using System Center 2012 Configuration Manager Service Pack 1. These services are expected to be available soon.

Opening Device Manager

You can open Device Manager in Windows 8 in a number of ways. The first method involves using the hotspot in the lower-left corner of the desktop. When you move your mouse pointer to that location or tap it, a small representation of the Start screen appears, as shown in Figure 3-2.

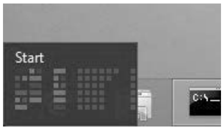


FIGURE 3-2 The hotspot in the lower-left corner of the desktop

On this miniature rendition of the Start screen, right-click or tap and hold to open the Power Users menu shown in Figure 3-3. The Device Manager tool appears on this menu.

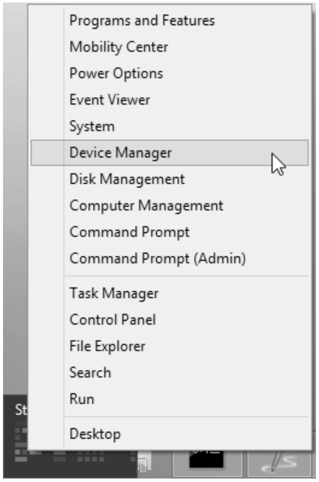


FIGURE 3-3 Power Users menu to access Device Manager

You can also open Device Manager by selecting the Settings charm from the Windows desktop and then selecting Control Panel. When Control Panel opens, start typing **Device Manager** in the Search box. Any items in Control Panel that match what you've typed will be displayed. In Figure 3-4, you can see that one of the first items that appears is Device Manager. To open it, click or tap Device Manager.

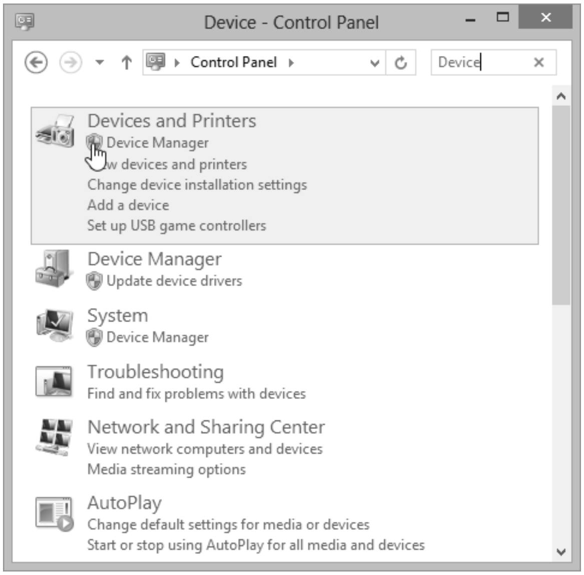

Device - Control Panel
Control Panel
Device
Devices and Printers
Device Manager
w devices and printers
Change device installation settings
Add a device
Set up USB game controllers
Device Manager
Update device drivers
System
Device Manager
Troubleshooting
Find and fix problems with devices
Network and Sharing Center
View network computers and devices
Media streaming options
AutoPlay
Change default settings for media or devices
Start or stop using AutoPlay for all media and devices

FIGURE 3-4 Opening Device Manager from Control Panel

A third way to open Device Manager is to open a command prompt and run the **devmgmt.msc** command. A fourth way is to open the Power Users menu, tap or click Run, type **devmgmt.msc**, and then tap or click OK.

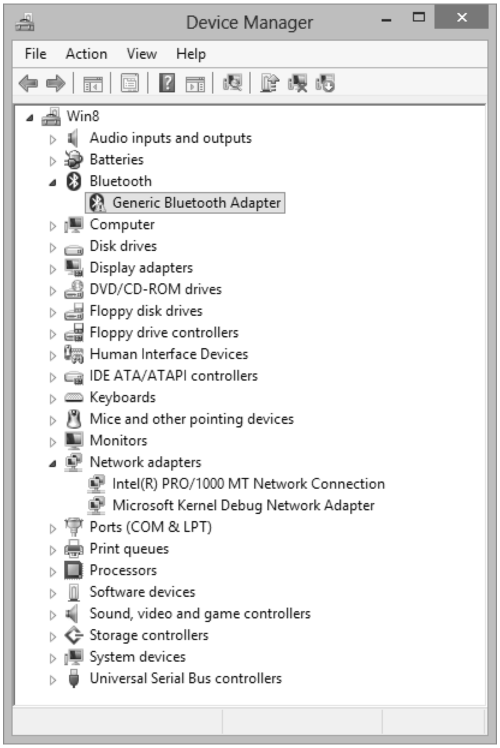
When you have opened Device Manager, you can perform a number of device-related and driver-related tasks, including the following:

- Viewing the status of a device
- Finding the version of a particular driver
- Updating a driver
- Reinstalling a driver
- Rolling back a driver to a previous version
- Enabling or disabling a device

You learn about these actions in this chapter.

Viewing device and driver information

The Device Manager window (Figure 3-5) is organized in a tree view with the computer name at the top of the window and individual device categories nested beneath.



- Win8
  - Audio inputs and outputs
  - Batteries
  - Bluetooth
    - Generic Bluetooth Adapter
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Floppy disk drives
  - Floppy drive controllers
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Intel(R) PRO/1000 MT Network Connection
    - Microsoft Kernel Debug Network Adapter
  - Ports (COM & LPT)
  - Print queues
  - Processors
  - Software devices
  - Sound, video and game controllers
  - Storage controllers
  - System devices
  - Universal Serial Bus controllers

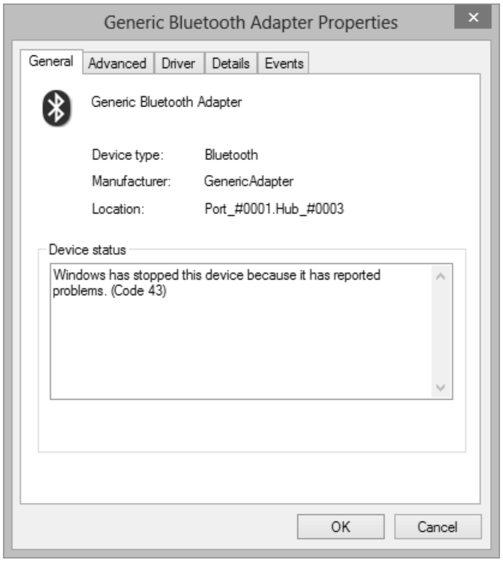
FIGURE 3-5 Device Manager in Windows 8

To view the details about a particular device, expand the appropriate hardware node and double-click or double-tap the device. This opens the Properties page for the device, like the one shown in Figure 3-6. There are several tabs; the tabs that you see depend on the particular device you open. The common tabs are as follows:

- General
- Advanced
- Driver
- Details
- Events

THE GENERAL TAB

The General tab provides you with a quick overview of the device, which includes the current status of the selected device. In Figure 3-6, you can see that this particular device is not functional because Windows automatically stopped the device due to too many errors.



Generic Bluetooth Adapter Properties

Generic Bluetooth Adapter

Device type: Bluetooth
Manufacturer: GenericAdapter
Location: Port_#0001.Hub_#0003

Device status

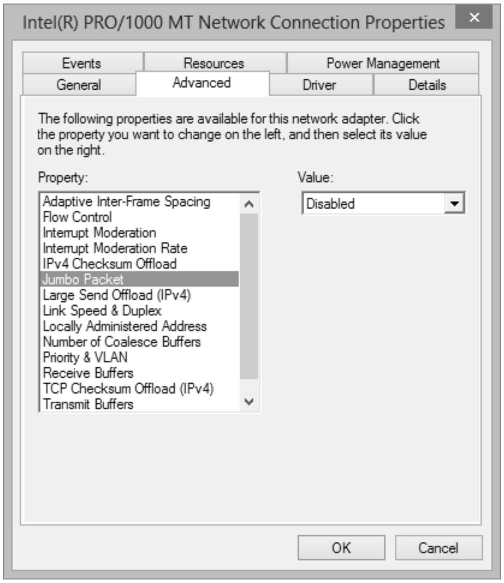
Windows has stopped this device because it has reported problems. (Code 43)

FIGURE 3-6 Properties for a failing Bluetooth device

THE ADVANCED TAB

Jumbo Packet in this configuration refers to the adopted standard Jumbo Frames technology. See this URL for more information: *http://www.ethernetalliance.org/wp-content/uploads/2011/10/EA-Ethernet-Jumbo-Frames-v0-1.pdf*.

If there are advanced configurable properties for the device, they appear on the Advanced tab, as shown in Figure 3-7. For the network adapter shown in this figure, there are advanced settings that control exactly how the device will behave on the network. In this case, Jumbo Packet is disabled. To enable it, select Enabled from the Value drop-down list. Available values change to whatever is appropriate for the selected property.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- Adaptive Inter-Frame Spacing
- Flow Control
- Interrupt Moderation
- Interrupt Moderation Rate
- IPv4 Checksum Offload
- Jumbo Packet
- Large Send Offload (IPv4)
- Link Speed & Duplex
- Locally Administered Address
- Number of Coalesce Buffers
- Priority & VLAN
- Receive Buffers
- TCP Checksum Offload (IPv4)
- Transmit Buffers

Value: Disabled

FIGURE 3-7 The Advanced tab in the Properties page for a network adapter

THE DRIVER TAB

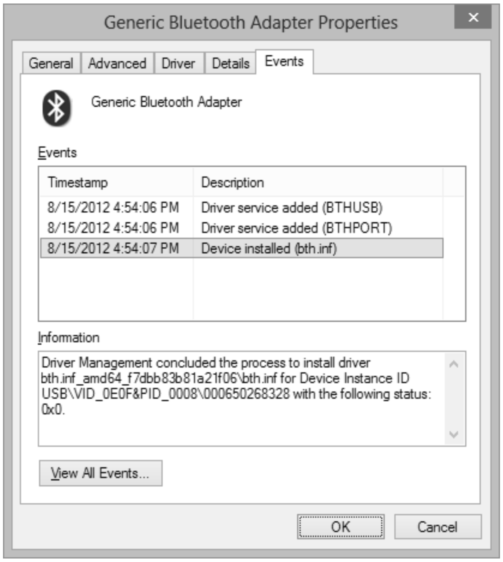
The Driver tab includes all the items necessary to fully manage the driver software for the selected device. You learn more about this tab in the “Managing drivers” section later in this chapter.

THE DETAILS TAB

You find information about the hardware on the Details tab. Every hardware device has information associated with it. There can be just a little information or quite a lot of information.

THE EVENTS TAB

The Events tab provides you with a list of system events associated with the device. In Figure 3-8, three events associated with the Bluetooth adapter have taken place. By clicking the View All Events button in this window, the Event Viewer opens and displays the events in context with other system operations. Not every device has an Events tab.



Generic Bluetooth Adapter

Events

Timestamp	Description
8/15/2012 4:54:06 PM	Driver service added (BTHUSB)
8/15/2012 4:54:06 PM	Driver service added (BTHPORT)
8/15/2012 4:54:07 PM	Device installed (bth.inf)

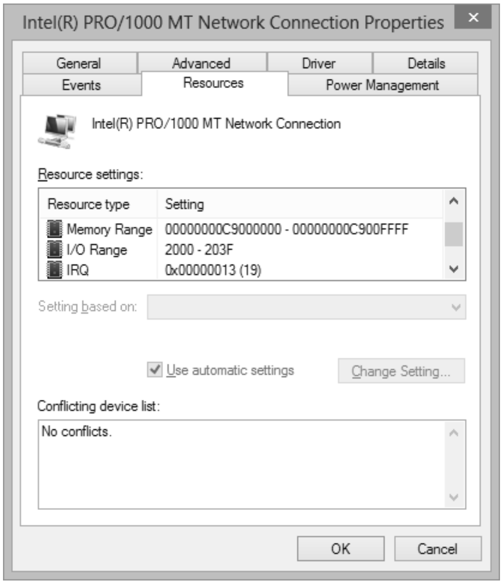
Information

Driver Management concluded the process to install driver bth.inf_amd64_f7dbb83b81a21f06\bth.inf for Device Instance ID USB\VID_0E0F&PID_0008\000650268328 with the following status: 0x0.

FIGURE 3-8 The Events tab for the Bluetooth adapter

THE RESOURCES TAB

Early in the days of information technology (pre–Windows 95), technology professionals had to configure each component's resource settings manually to ensure that there were no resource conflicts and that all devices had the resources they needed to operate. In Figure 3-9, you can see the resources the hardware device is using.



Intel(R) PRO/1000 MT Network Connection

Resource settings:

Resource type	Setting
Memory Range	00000000C9000000 - 00000000C900FFFF
I/O Range	2000 - 203F
IRQ	0x00000013 (19)

Setting based on:

☑ Use automatic settings

Conflicting device list:

No conflicts.

FIGURE 3-9 Resources in use by the selected device

The resource types include Memory Range, I/O Range, and IRQ.

- Most devices require some memory. The Memory Range setting on the Resources tab identifies the memory location the hardware device is using.
- The I/O Range setting is reserved and helps the hardware device communicate with the system.
- The IRQ stetting is for the *Interrupt Request line (IRQ)*. A system has a predefined number of IRQs available. An IRQ provides a device that can interrupt system operations to service the needs of the configured hardware device.

If it is necessary to change a device's default configuration, clear the Use Automatic Settings check box and tap or click Change Setting; you can then provide new information for the device.

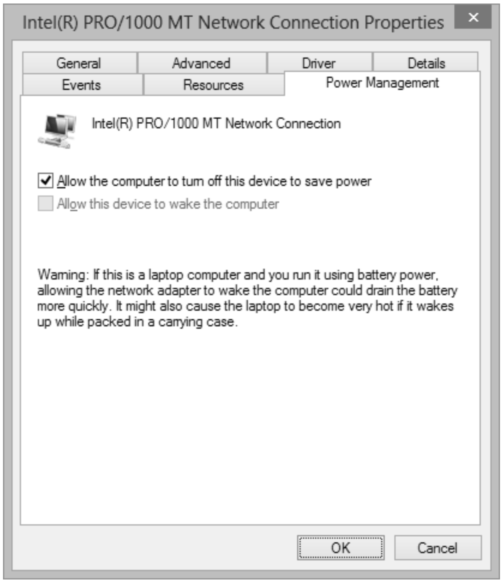
REAL WORLD **THE DEFAULT DEVICE CONFIGURATION IS ALMOST ALWAYS FINE**

Although there was a day when administrators manually modified all the settings you just learned about, those days are all but over. In almost every situation, devices are added to Windows with a default configuration that just works. Today's systems have evolved to a point that resource assignments are usually automatic. However, for troubleshooting purposes, you should have at least a basic understanding of these items in the event that you do find a system that is experiencing some kind of conflict requiring manual resolution.

Managing drivers

You can manage the power of some devices to reduce the amount of electricity they use. This can lower power bills and is especially useful for extending the battery life of a portable device. In Figure 3-10, note that there is an Allow The Computer To Turn Off This Device To Save Power check box. Clear the check box to prevent the system from turning off this device.

At times, the computer will go to sleep but can be awakened through various means such as opening a laptop lid or pressing the power button or a key on the keyboard. For devices that can wake up the computer to perform operations, the Allow This Device To Wake The Computer check box can also be selected.


Intel(R) PRO/1000 MT Network Connection Properties

Intel(R) PRO/1000 MT Network Connection

☑ Allow the computer to turn off this device to save power

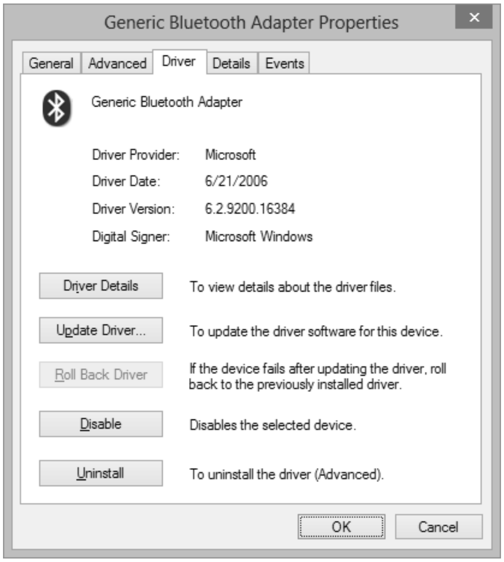
□ Allow this device to wake the computer

Warning: If this is a laptop computer and you run it using battery power, allowing the network adapter to wake the computer could drain the battery more quickly. It might also cause the laptop to become very hot if it wakes up while packed in a carrying case.

FIGURE 3-10 Power management configuration for the network adapter

As mentioned previously, the Driver tab (Figure 3-11) contains a number of options for managing the drivers associated with a device. On this tab, you can get some details about the driver in use, including the name of the company that provided the driver, the date that the driver was last updated, the driver version, and the name of the company that digitally signed the driver.

Perhaps the most important details here are the driver provider and driver version data. When you’re troubleshooting an issue related to hardware, you will want to ensure that you’re using the latest drivers that are available for the device. This is generally considered the first troubleshooting step for hardware problems.



Generic Bluetooth Adapter Properties

Generic Bluetooth Adapter

Driver Provider: Microsoft
Driver Date: 6/21/2006
Driver Version: 6.2.9200.16384
Digital Signer: Microsoft Windows

To view details about the driver files.

To update the driver software for this device.

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

Disables the selected device.

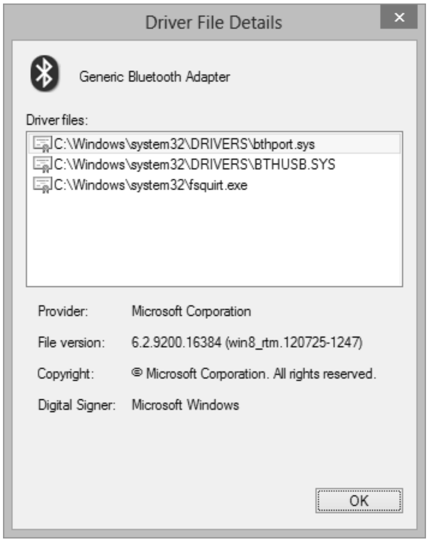
To uninstall the driver (Advanced).

FIGURE 3-11 Driver information for the Bluetooth adapter

A number of options are available on the Driver tab, but this section focuses on just three. The Disable and Uninstall options are self-explanatory.

DRIVER DETAILS

Select Driver Details to display information about the driver associated with the currently selected device. Like the Driver tab, this informational page displays the driver version. It also shows you all the files that are associated with the driver. In Figure 3-12, you can see that the Bluetooth adapter has three files associated with it.



Driver File Details

Generic Bluetooth Adapter

Driver files:

```
C:\Windows\system32\DRIVERS\bthport.sys
C:\Windows\system32\DRIVERS\BTHUSB.SYS
C:\Windows\system32\fsquirt.exe
```

Provider: Microsoft Corporation
File version: 6.2.9200.16384 (win8_rtm.120725-1247)
Copyright: © Microsoft Corporation. All rights reserved.
Digital Signer: Microsoft Windows

FIGURE 3-12 File information for the selected driver

UPDATE DRIVER

You learned that a first troubleshooting step is often ensuring that a device's driver files are the most current ones available. Here's how you update a driver:

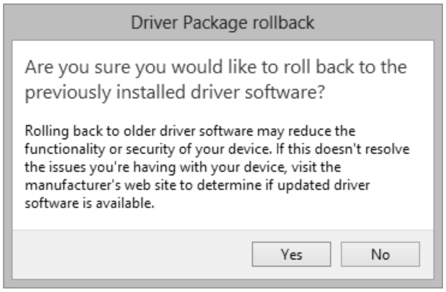
1. On the Driver tab, tap or click Update Driver.
2. Decide how the driver should be updated and select one of the following options:
   - Search Automatically For Updated Driver Software Selecting this option instructs Windows to search both your local computer and the Internet for new drivers.
   - Browse My Computer For Driver Software If you've manually downloaded an updated driver for a hardware device, choose this option to direct Windows to the download location and install the updated driver software.
3. When you complete these steps, the new driver is installed, and the version number is updated.

> ***REAL WORLD*** **DRIVER INSTALLATION PACKAGES**
>
> **For some hardware, it might be necessary to use Driver Manager to install updated drivers. However, for many hardware devices, hardware vendors provide installation packages that make the driver update process a bit easier. This is especially true for graphics cards vendors such as Nvidia and BFG, who release new update packages on a regular basis. For these kinds of hardware, when you download the update package from the vendor and run the installation package, the drivers are also updated.**

ROLL BACK DRIVER

As is the case with any software package, bad code or security flaws can occasionally be introduced in drivers that create system instability or that compromise system security. In these cases, you might find it necessary to revert to an earlier driver that worked.

This is the reason that the driver rollback feature exists in Device Manager on the Driver tab. If it is necessary to revert to a previous driver, Windows warns you (Figure 3-13) that you might experience problems, including reduced security and functionality. It's recommended that you roll back a driver only if you're experiencing a driver-related hardware issue.



Driver Package rollback

Are you sure you would like to roll back to the previously installed driver software?

Rolling back to older driver software may reduce the functionality or security of your device. If this doesn't resolve the issues you're having with your device, visit the manufacturer's web site to determine if updated driver software is available.

FIGURE 3-13 Roll back a driver only if necessary

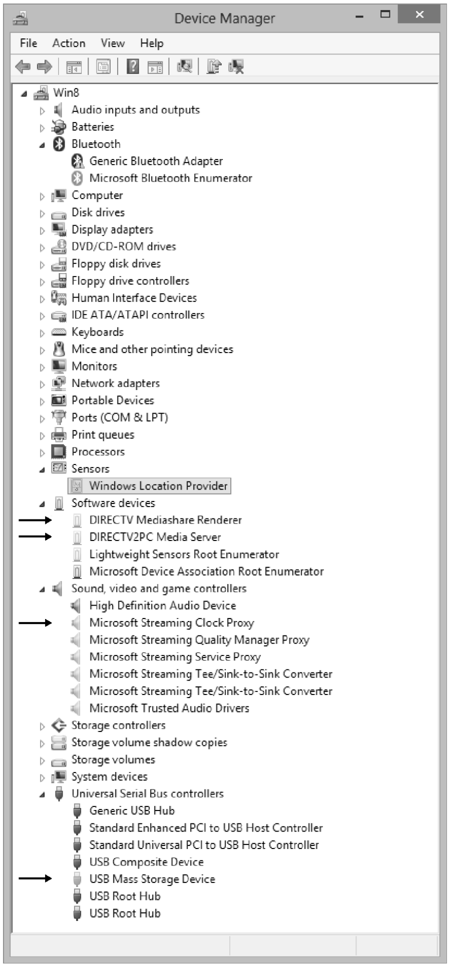
Displaying hidden devices

In some troubleshooting scenarios, you might want to display devices that the system has marked as hidden in the registry. By default, Device Manager does not display information for hidden devices.

To enable Device Manager to display devices that are marked as hidden:

1. Open Device Manager.
2. From the View menu, choose Show Hidden Devices.

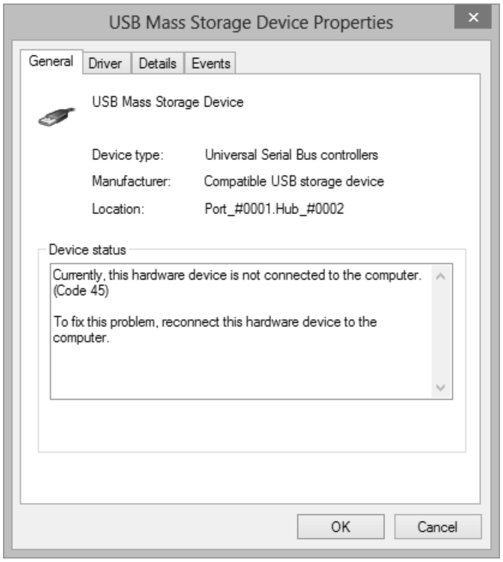
In Figure 3-14, note that the Device Manager view now includes a number of additional nodes and devices that did not appear before. Although it might be difficult to see, the hidden devices are displayed in a dimmed font in the Device Manager view.



```
Win8
  Audio inputs and outputs
  Batteries
  Bluetooth
    Generic Bluetooth Adapter
    Microsoft Bluetooth Enumerator
  Computer
  Disk drives
  Display adapters
  DVD/CD-ROM drives
  Floppy disk drives
  Floppy drive controllers
  Human Interface Devices
  IDE ATA/ATAPI controllers
  Keyboards
  Mice and other pointing devices
  Monitors
  Network adapters
  Portable Devices
  Ports (COM & LPT)
  Print queues
  Processors
  Sensors
    Windows Location Provider
  Software devices
    DIRECTV Mediashare Renderer
    DIRECTV2PC Media Server
    Lightweight Sensors Root Enumerator
    Microsoft Device Association Root Enumerator
  Sound, video and game controllers
    High Definition Audio Device
    Microsoft Streaming Clock Proxy
    Microsoft Streaming Quality Manager Proxy
    Microsoft Streaming Service Proxy
    Microsoft Streaming Tee/Sink-to-Sink Converter
    Microsoft Streaming Tee/Sink-to-Sink Converter
    Microsoft Trusted Audio Drivers
  Storage controllers
  Storage volume shadow copies
  Storage volumes
  System devices
  Universal Serial Bus controllers
    Generic USB Hub
    Standard Enhanced PCI to USB Host Controller
    Standard Universal PCI to USB Host Controller
    USB Composite Device
    USB Mass Storage Device
    USB Root Hub
    USB Root Hub
```

FIGURE 3-14 Hidden devices shown slightly dimmed

After you are able to view hidden devices, you can manage them as you would any other device. When you select a hidden device, you can see why the device is hidden. In Figure 3-15, note that the device is hidden from Device Manager because it's not currently connected to the computer. This is often the case for USB mass storage devices, which include portable thumb drives.



USB Mass Storage Device

Device type: Universal Serial Bus controllers

Manufacturer: Compatible USB storage device

Location: Port_#0001.Hub_#0002

Device status

Currently, this hardware device is not connected to the computer. (Code 45)

To fix this problem, reconnect this hardware device to the computer.

FIGURE 3-15 A device not currently connected to the computer

Using the System Information utility

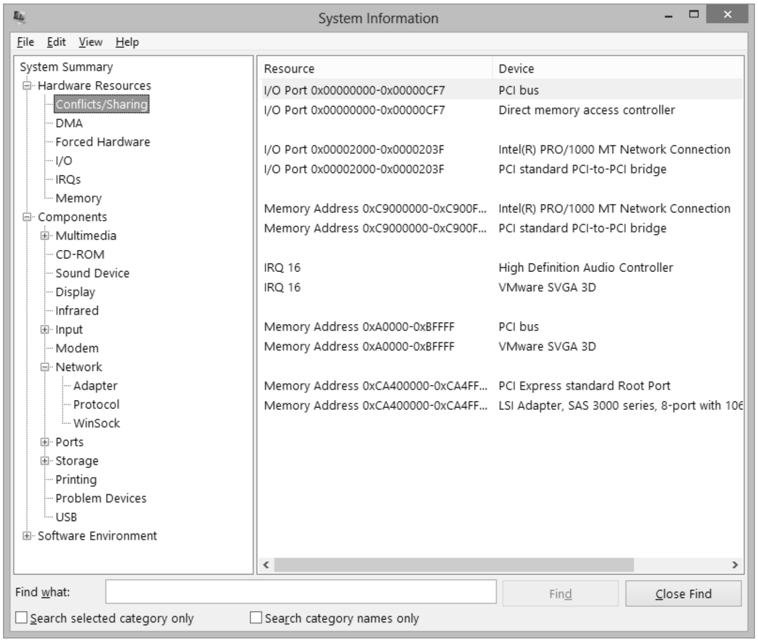
The Device Manager utility provides you with a way to view and manipulate your hardware and the enabling software drivers. It's a read/write utility in that you can make changes to the system. However, that might be more than you need. Sometimes, you just need to view a lot of information all at once, even if you cannot make changes to the information. That's where the System Information utility is useful.

The System Information utility displays a plethora of information about your system that is read-only. You can't change any of the information. By using this utility, you can view details about hardware resources, system components, and the software environment.

To access the System Information utility, type **msinfo32** on the Start screen, and then tap or click the resulting entry.

Viewing conflicting or shared resources

With Device Manager, identifying resource conflicts or identifying devices that are sharing resources requires you to open details for every device. In the System Information utility, identifying these situations is as easy as selecting System Summary, Hardware Resources, and then Conflicts/Sharing. As you can see in Figure 3-16, the System Information utility makes it easier to see this information.



Resource	Device
I/O Port 0x00000000-0x00000CF7	PCI bus
I/O Port 0x00000000-0x00000CF7	Direct memory access controller
I/O Port 0x00002000-0x0000203F	Intel(R) PRO/1000 MT Network Connection
I/O Port 0x00002000-0x0000203F	PCI standard PCI-to-PCI bridge
Memory Address 0xC9000000-0xC900F...	Intel(R) PRO/1000 MT Network Connection
Memory Address 0xC9000000-0xC900F...	PCI standard PCI-to-PCI bridge
IRQ 16	High Definition Audio Controller
IRQ 16	VMware SVGA 3D
Memory Address 0xA0000-0xBFFFF	PCI bus
Memory Address 0xA0000-0xBFFFF	VMware SVGA 3D
Memory Address 0xCA400000-0xCA4FF...	PCI Express standard Root Port
Memory Address 0xCA400000-0xCA4FF...	LSI Adapter, SAS 3000 series, 8-port with 106

FIGURE 3-16 Viewing resource sharing and conflict information

Note that resource sharing and conflicts are not necessarily bad things. A number of years ago, administrators had to make sure that resource sharing never occurred, but modern systems use limited system resources much more efficiently by sharing these resources when it makes sense to do so.

System Information highlights

So much information is available in this utility that it's not possible to show everything in just a few pages. Take the time to review the System Information utility and get familiar with it. It contains a lot of information that you will find useful. Highlights of the utility are shown in Table 3-1.

TABLE 3-1 The System Information utility

Path	Description
Components, Network, Adapter	Displays a list of all the network adapters installed in the system along with all the configuration information related to each adapter, including IP address, DHCP lease information, adapter model, and MAC address
Components, Problem Devices	Displays a list of the devices that are currently experiencing some kind of problem and that need attention

Path	Description
Software Environment, Network Connections	Displays a list of network resources to which the local system is connected
Software Environment, Running Tasks	Displays a list of all running tasks along with the full path to the related executable, the process ID, software version, and size
Software Environment, Environment Variables	Displays a list of all the environment variables that have been created on the system

Discovering the Driver Verifier utility

Starting with Windows 2000, Windows has included a Driver Verifier utility intended for use by advanced users in troubleshooting particularly vexing driver-related issues. The Driver Verifier utility helps determine root cause for driver-related issues, including problems related to:

- Drivers that experience memory-based issues
- Poorly written drivers
- Drivers that cause the system to fail

IMPORTANT **POTENTIAL PERFORMANCE ISSUES**

The Driver Verifier utility can create system instability and performance issues. Use this tool with care and only after fully reviewing the documentation so that you are confident that you understand what is happening. The system is likely to fail more often while the Driver Verifier utility is collecting information and generating dump files that can be analyzed later.

Initializing a new Driver Verifier configuration requires you to restart your system for the configuration changes to take effect.

Table 3-2 lists the standard tests the Driver Verifier utility can perform.

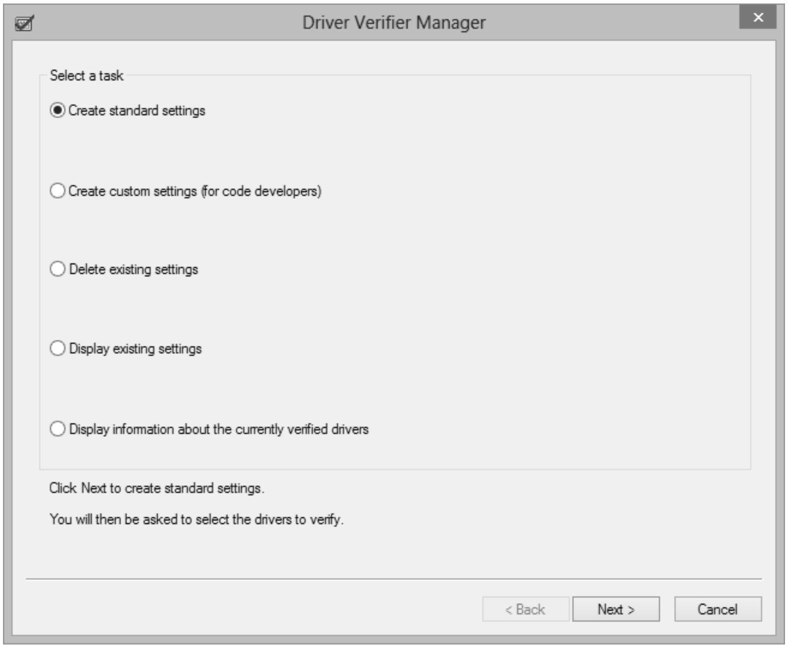
TABLE 3-2 Standard tests

Test	Description
Special pool	When activated, selected driver memory is pulled from a special pool, which is monitored for memory overruns, memory underruns, and memory that is accessed after it is freed.
Pool tracking	A method for detecting memory leaks. Ensures that a driver returns all its memory after it is unloaded.
Force IRQL checking	Places a driver under pressure in an attempt to make the driver access paged memory at the wrong IRQL. (Interrupt Request Level is the priority of an interrupt request.)
I/O verification	Monitors the way a driver handles I/O to detect illegal or inconsistent use of I/O routines.

Test	Description
Deadlock detection	Detects whether the driver has the potential to cause a deadlock. A deadlock occurs when two or more threads conflict over a resource, thwarting execution.
DMA checking	Detects a driver's improper use of Direct Memory Access (DMA) buffers, adapters, and map registers.
Security checks	Enables Driver Verifier to look for common situations that can result in driver-based security vulnerabilities.
Force pending I/O requests	Ensures that pending I/O requests are handled.
Low resources simulation	Tests a driver's ability to cope with low-resource situations, which can create resource contention issues.
IRP logging	Monitors a driver's use of IRPs (I/O request packets).
Miscellaneous checks	Many common items create driver instability. This category catches these common items.
Invariant MDL checking for stack	Monitors how the driver handles invariant MDL buffers across the driver stack.
Invariant MDL checking for driver	Monitors how the driver handles invariant MDL buffers per driver.
Power framework delay fuzzing	Helps identify driver errors for drivers that use the system's power framework.
DDI compliance checking	Determines whether the driver interacts correctly with the Windows kernel.

You can use the Driver Verifier utility in one of two ways. If you want to use the tool from a command line, type **verifier** followed by a valid verifier command. If you want to use a GUI-based version of the tool, type **verifier** from a command line. In this section, you learn about the GUI-based tool.

1. At a command prompt, type **verifier** to open the Driver Verifier Manager (GUI-based tool), as shown in Figure 3-17.



Select a task

● Create standard settings

○ Create custom settings (for code developers)

○ Delete existing settings

○ Display existing settings

○ Display information about the currently verified drivers

Click Next to create standard settings.

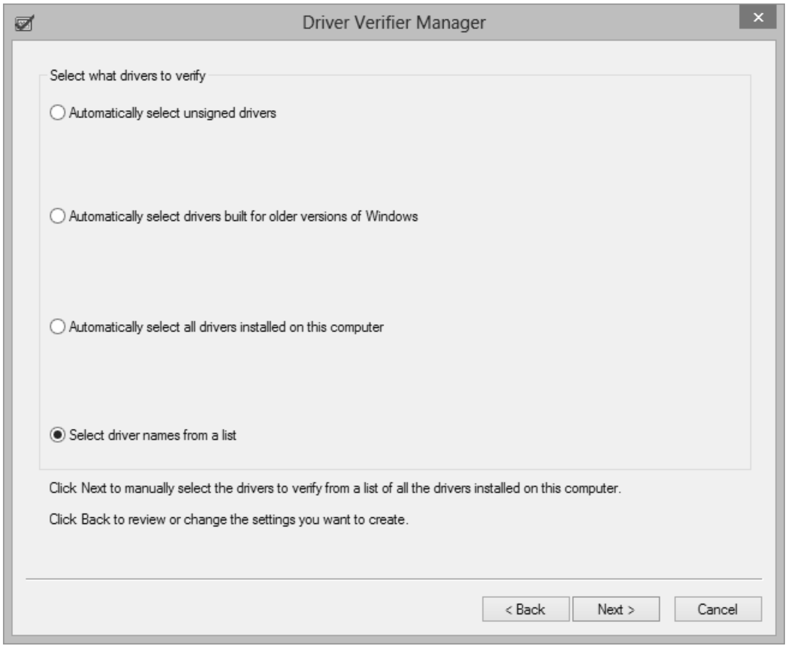
You will then be asked to select the drivers to verify.

FIGURE 3-17 The Driver Verifier utility

The available tasks are:

- **Create Standard Settings** This task selects a standard set of options and then asks you to select the drivers that are to be verified.
- **Create Custom Settings** With this task, you choose the Driver Verifier tests that should be run against the drivers you choose.
- **Delete Existing Settings** This task deactivates any Driver Verifier settings that are in place. It’s important to remember that Driver Verifier settings remain in place until you actively delete them.
- **Display Existing Settings** This task displays the settings that will be activated and the list of drivers that will be affected.
- **Display Information About The Currently Verified Drivers** This task displays information about the actions Driver Verifier is performing.

2. Select the Create Standard Settings option and tap or click Next. The Driver Verifier Manager displays the page, shown in Figure 3-18, on which you identify which drivers you want to verify.



Select what drivers to verify

○ Automatically select unsigned drivers

○ Automatically select drivers built for older versions of Windows

○ Automatically select all drivers installed on this computer

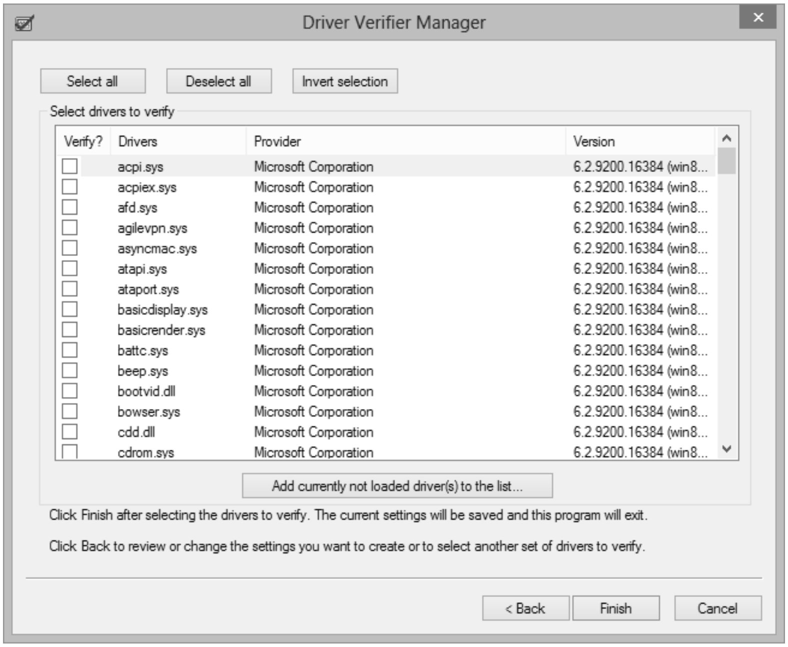
● Select driver names from a list

Click Next to manually select the drivers to verify from a list of all the drivers installed on this computer.

Click Back to review or change the settings you want to create.

FIGURE 3-18 Choosing the drivers that are to be verified

3. Select the Select Driver Names From A List option and tap or click Next. Driver Verifier Manager displays the page shown in Figure 3-19.



Select drivers to verify

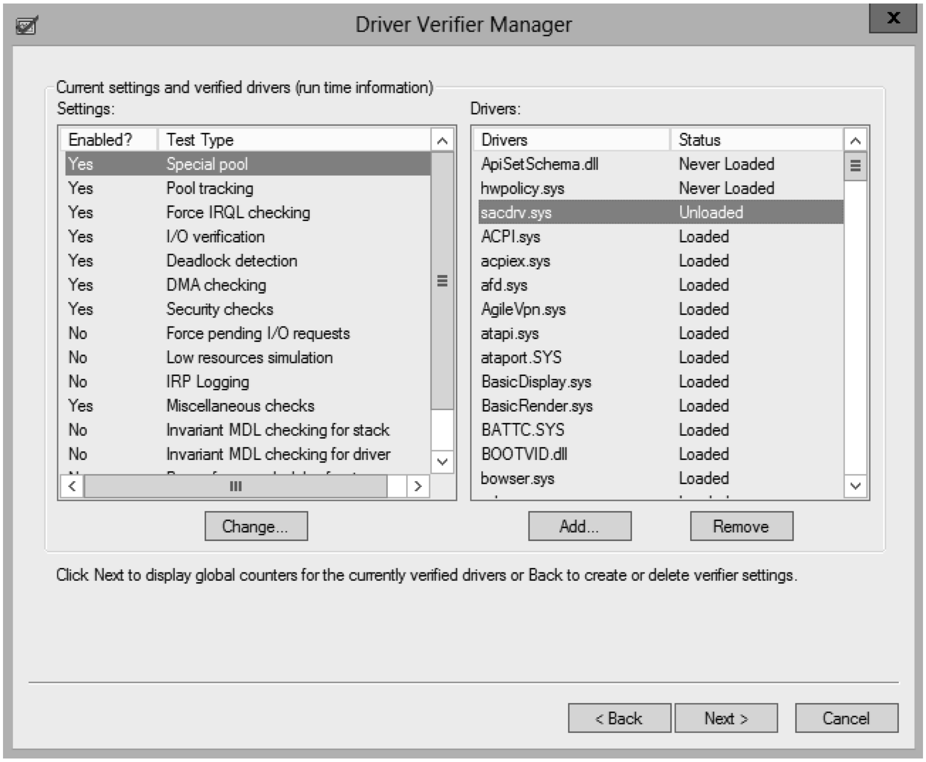
Verify?	Drivers	Provider	Version
□	acpi.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	acpiex.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	afd.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	agilevpn.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	asyncmac.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	atapi.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	ataport.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	basicdisplay.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	basicrender.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	battc.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	beep.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	bootvid.dll	Microsoft Corporation	6.2.9200.16384 (win8...
□	bowser.sys	Microsoft Corporation	6.2.9200.16384 (win8...
□	cdd.dll	Microsoft Corporation	6.2.9200.16384 (win8...
□	cdrom.sys	Microsoft Corporation	6.2.9200.16384 (win8...

Click Finish after selecting the drivers to verify. The current settings will be saved and this program will exit.

Click Back to review or change the settings you want to create or to select another set of drivers to verify.

FIGURE 3-19 Selecting the drivers that are to be verified

4. Select the drivers you want to verify and then tap or click Finish.
5. You will probably have to restart your system. After the computer restarts, load the Driver Verifier GUI again. Choose Display Information About The Currently Verified Drivers and click Next. Driver Verifier Manager presents the current settings and verified drivers, including the status of every driver, as shown in Figure 3-20.



Driver Verifier Manager

Current settings and verified drivers (run time information)

Settings:

Enabled?	Test Type
Yes	Special pool
Yes	Pool tracking
Yes	Force IRQL checking
Yes	I/O verification
Yes	Deadlock detection
Yes	DMA checking
Yes	Security checks
No	Force pending I/O requests
No	Low resources simulation
No	IRP Logging
Yes	Miscellaneous checks
No	Invariant MDL checking for stack
No	Invariant MDL checking for driver

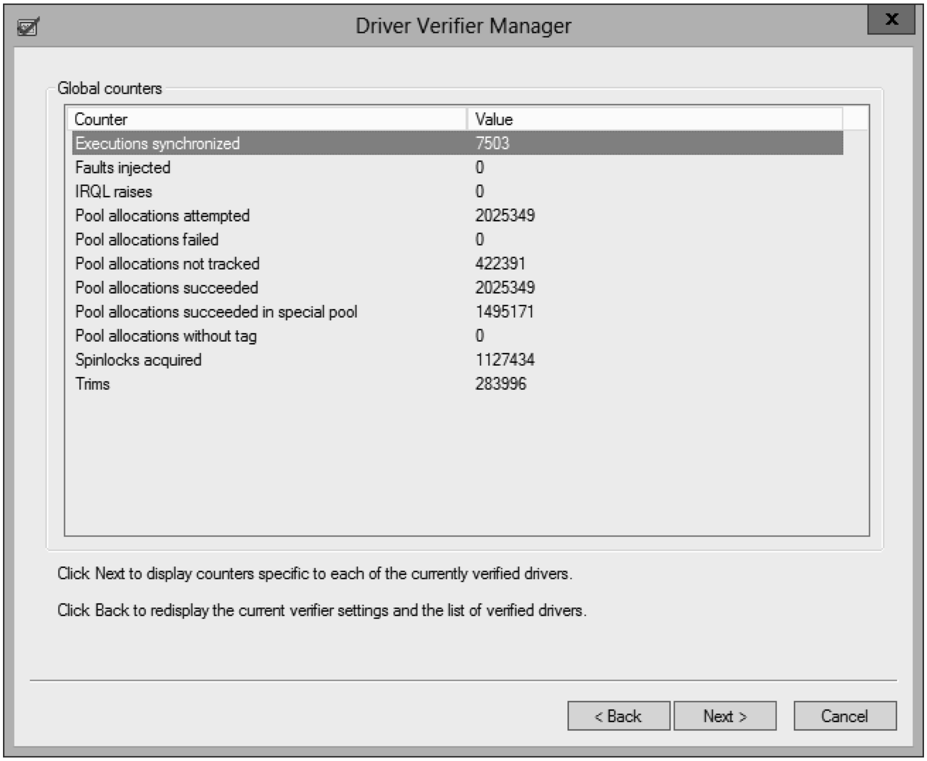
Drivers:

Drivers	Status
ApiSetSchema.dll	Never Loaded
hwpolicy.sys	Never Loaded
sacdrv.sys	Unloaded
ACPI.sys	Loaded
acpiex.sys	Loaded
afd.sys	Loaded
AgileVpn.sys	Loaded
atapi.sys	Loaded
ataport.SYS	Loaded
BasicDisplay.sys	Loaded
BasicRender.sys	Loaded
BATTC.SYS	Loaded
BOOTVID.dll	Loaded
bowser.sys	Loaded

Click Next to display global counters for the currently verified drivers or Back to create or delete verifier settings.

FIGURE 3-20 Driver Verifier Manager running and loading drivers

6. To view the global counter information for the verified drivers, click Next to see the global counter information, as shown in Figure 3-21.



Driver Verifier Manager

Global counters

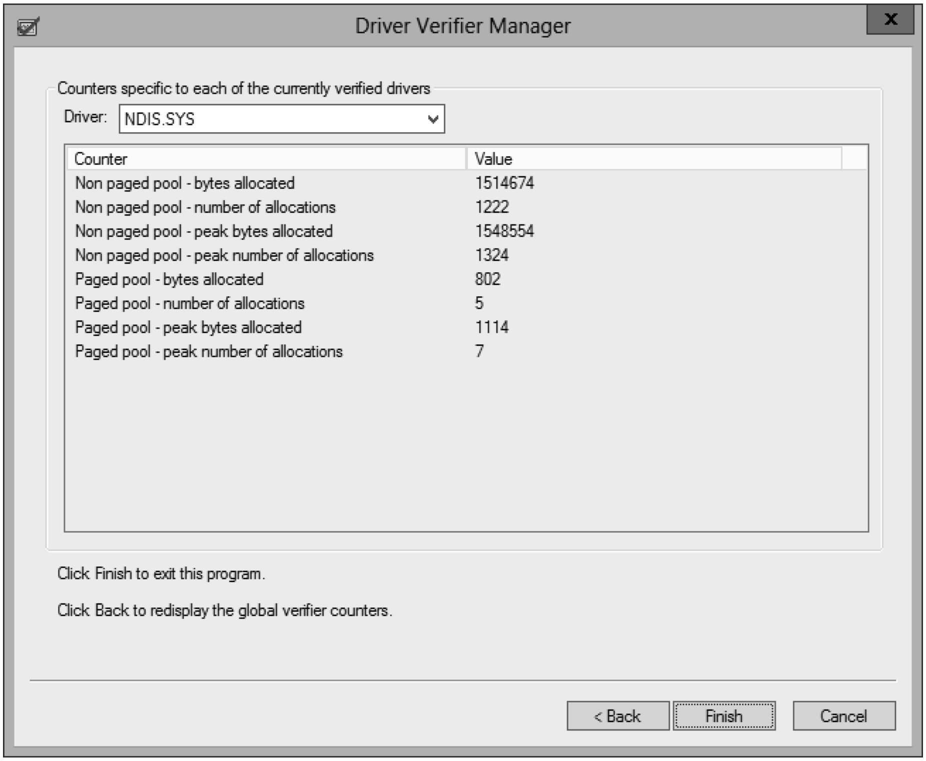
Counter	Value
Executions synchronized	7503
Faults injected	0
IRQL raises	0
Pool allocations attempted	2025349
Pool allocations failed	0
Pool allocations not tracked	422391
Pool allocations succeeded	2025349
Pool allocations succeeded in special pool	1495171
Pool allocations without tag	0
Spinlocks acquired	1127434
Trims	283996

Click Next to display counters specific to each of the currently verified drivers.

Click Back to redisplay the current verifier settings and the list of verified drivers.

FIGURE 3-21 The Driver Verifier Manager global counters page

7. Click Next to move to the page, shown in Figure 3-22, on which you can select an individual driver to view its specific information. In Figure 3-22, the NDIS.SYS driver—which is linked to the networking component—is the selected driver, and its counter information is displayed.



Counters specific to each of the currently verified drivers

Driver: NDIS.SYS

Counter	Value
Non paged pool - bytes allocated	1514674
Non paged pool - number of allocations	1222
Non paged pool - peak bytes allocated	1548554
Non paged pool - peak number of allocations	1324
Paged pool - bytes allocated	802
Paged pool - number of allocations	5
Paged pool - peak bytes allocated	1114
Paged pool - peak number of allocations	7

Click Finish to exit this program.

Click Back to redisplay the global verifier counters.

FIGURE 3-22 Driver Verifier Manager details for NDIS.SYS

8. Click Finish.

MORE INFO **DRIVER VERIFIER UTILITY FACTS**

To learn more about the Driver Verifier utility, review these resources, which go into great detail about how this utility operates and how to interpret the results:

- *http://support.microsoft.com/kb/244617*
- *http://msdn.microsoft.com/en-us/library/windows/hardware/ff545470(v=vs.85).aspx*

Make sure you understand that the driver utility only helps you track down a problem, not necessarily resolve it. Most driver issues identified by the driver utility must be rewritten to be fixed. Because you probably won't have the source code for the driver, you must work with the vendor to fix the driver, download a new driver, or use a different hardware device.

Adding device drivers to the driver store

In an enterprise environment, it can be important to preinstall drivers on a computer before deploying it in the organization. It's not uncommon for desktop administrators to make sure that all the drivers that a user would need are preloaded on the system. By doing so, when a user plugs in a supported device, the drivers are available and the device works for the user without any difficulty.

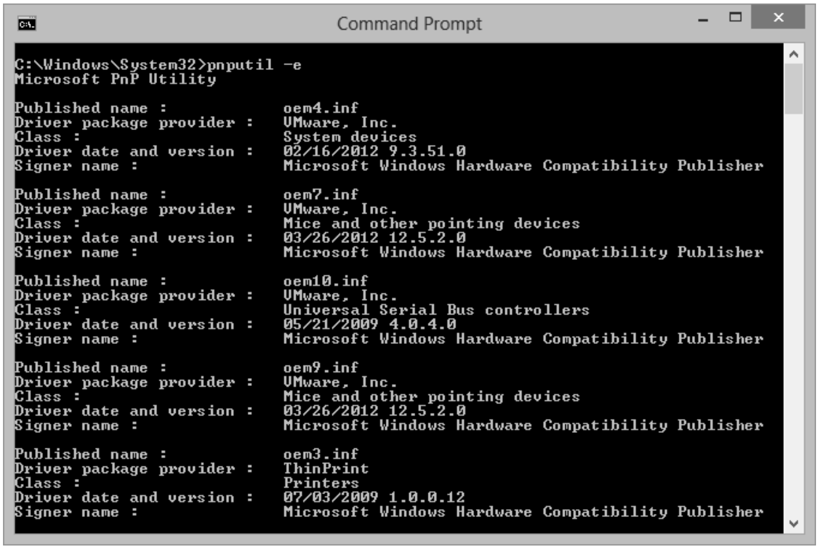
Windows includes a command-line tool called Pnputil.exe which you use to manage the driver store with a number of parameters, listed in Table 3-3.

TABLE 3-3 Pnputil.exe parameters

Parameter	Description
pnputil -a	Adds a driver package to the driver store.
pnputil -i	(Used with -a) If the driver matches any existing hardware devices on the system, the driver software will be installed.
pnputil -e	Shows you a list of third-party drivers currently loaded in the driver store.
pnputil -d	Deletes a package from the driver store.
pnputil -f	(Used with -d) Forces the deletion of a package from the driver store. The parameter is required when a driver you want to delete is associated with a device that is still connected to the system.

Sample commands:

- **pnputil -a c:\NewDriver.inf** Loads the NewDriver.inf driver located in C drive into the driver store.
- **pnputil -d oem3.inf** On the sample system used for this chapter, removes the driver associated with the VMware ThinPrint service.
- **pnputil -e** Shows you a list of the third-party drivers currently loaded on the system (Figure 3-23).



```
C:\Windows\System32>pnputil -e
Microsoft PnP Utility

Published name :            oem4.inf
Driver package provider :   VMware, Inc.
Class :                     System devices
Driver date and version :   02/16/2012 9.3.51.0
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem7.inf
Driver package provider :   VMware, Inc.
Class :                     Mice and other pointing devices
Driver date and version :   03/26/2012 12.5.2.0
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem10.inf
Driver package provider :   VMware, Inc.
Class :                     Universal Serial Bus controllers
Driver date and version :   05/21/2009 4.0.4.0
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem9.inf
Driver package provider :   VMware, Inc.
Class :                     Mice and other pointing devices
Driver date and version :   03/26/2012 12.5.2.0
Signer name :               Microsoft Windows Hardware Compatibility Publisher

Published name :            oem3.inf
Driver package provider :   ThinPrint
Class :                     Printers
Driver date and version :   07/03/2009 1.0.0.12
Signer name :               Microsoft Windows Hardware Compatibility Publisher
```

FIGURE 3-23 A list of the third-party drivers loaded on the system

Lesson summary

- Drivers are the software glue that connects the operating system to the hardware devices.
- The Device Manager tool is used to manage all aspects of driver software in Windows 8.
- The Driver Verifier utility helps pinpoint potential driver issues that could be causing system instability.
- By adding drivers to the Driver Store, you can help employees more easily add new devices to their computers.
- You might have to roll back a driver to a previous version if a newer driver is unstable.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which tool provides you with read-only access to a variety of system information elements?

   A. Device Manager

   B. Driver Verifier

    C. System Information
    D. Computer Management
2. How do you enable the viewing of hidden devices?
    A. In View, choose Hidden Devices in Driver Verifier.
    B. Open Device Manager, choose View, and then select Show Hidden Devices.
    C. Right-click a device category and choose Show Hidden Devices.
    D. Open System Information and navigate to the Hidden Devices node.
3. Which of these methods does not update drivers?
    A. Driver Verifier
    B. Windows Update
    C. Driver pre-staging
    D. Internet download

Lesson 2: Managing hardware devices

Drivers are the software that binds the operating system to the hardware connected to the system. Drivers bring you to the focus of this chapter, which is the hardware.

After this lesson, you will be able to:

- Enable and disable hardware devices by using Device Manager.
- Monitor the amount of power USB devices use.

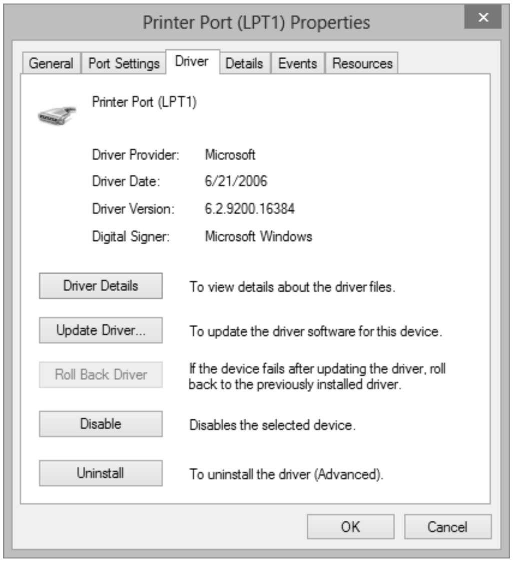
Estimated lesson time: 20 minutes

Enabling and disabling hardware devices

Not all hardware has to be enabled all the time. In fact, as you work on troubleshooting hardware in your organization, you might find it necessary to disable a device if it is causing problems. Then, after you correct a problem, you must bring the device back into operation.

To disable and enable devices, open the Device Manager by using one of the methods discussed previously in this chapter. Open the Properties page for the device you want to enable or disable and navigate to the Driver tab. From there, click either the Disable button (if the device is presently enabled) or the Enable button (if the device is presently disabled).

In Figure 3-24, note that the Disable button is currently available.



Printer Port (LPT1)

Driver Provider: Microsoft
Driver Date: 6/21/2006
Driver Version: 6.2.9200.16384
Digital Signer: Microsoft Windows

Driver Details: To view details about the driver files.
Update Driver...: To update the driver software for this device.
Roll Back Driver: If the device fails after updating the driver, roll back to the previously installed driver.
Disable: Disables the selected device.
Uninstall: To uninstall the driver (Advanced).

FIGURE 3-24 Disabling devices that are causing problems

Monitoring USB devices

Most devices that employees in your organization attach to their computers are USB-based. Such devices include keyboards, mice, cameras, and thumb drives. USB is so popular because it’s so easy to use. In many cases, all you have to do is plug in the device, and it just works. This is for two reasons. First, many common devices already have generic drivers loaded in Windows. When the device is plugged in, Windows already knows how to handle the hardware. Second, USB ports, in addition to enabling communication between the device and the computer, also provide power to the connected device. That’s why you don’t need to plug a thumb drive into a power source when you connect it to the computer.

Although some of the devices you use are connected directly to USB ports in the computer, others might be connected through a USB hub. There are two varieties of USB hubs:

- **Self-powered** A self-powered USB hub has a power supply that connects to an electrical outlet. These kinds of USB hubs provide their own power to connected devices.
- **Bus-powered** A bus-powered USB hub gets its power from the system’s USB connectors and passes along that power to connected devices. The amount of available power in this scenario is more limited than it is with self-powered hubs.

USB devices can operate at multiple speeds, and each speed is based on a different USB standard. Different devices conform to different standards. Modern computers often include USB ports that operate at multiple speeds. For example, a single computer might include ports that operate at both USB 2.0 and USB 3.0 speeds. Here's a look at the different standards and the speeds at which each operates:

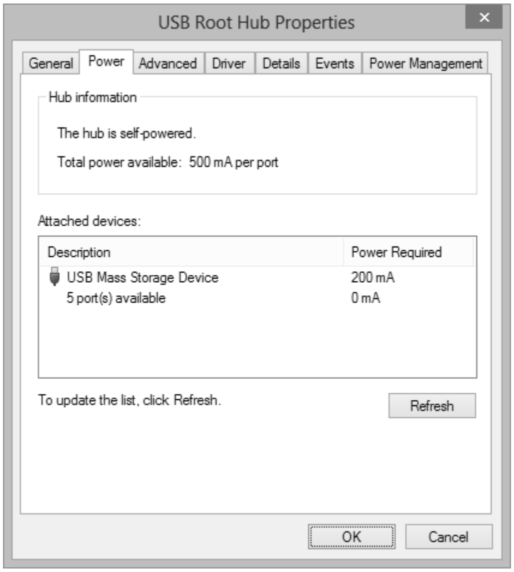
- **USB 1.0/USB 1.1** Operates at a maximum speed of 12 megabits per second (Mbps)
- **USB 2.0** Operates at a maximum speed of 480 Mbps
- **USB 3.0** Operates at a maximum speed of 5 gigabits per second (Gbps)

Bandwidth is an important factor in USB troubleshooting, particularly when you're dealing with older USB 1.0 or USB 1.1 systems. If there isn't sufficient bandwidth to support the devices on a particular USB port, users can receive error messages such as "USB controller bandwidth exceeded." When this happens, devices might not operate correctly.

Many devices will report to Windows the amount of bandwidth they use on the Advanced tab of the device's Properties page in Device Manager. However, this is not true for all devices. This makes troubleshooting bandwidth issues a best-effort task rather than a scientific one. Fortunately, with the rise of USB 3.0 and a maximum bandwidth of 5 GHz, bandwidth issues are not as serious as they once were.

As mentioned previously, USB devices consume power from the USB bus. Therefore, it's important to watch the USB port's power budget to ensure that connected devices don't surpass the power limit on the port. When you use a bus-powered USB hub to connect many devices, the possibility of exceeding this limit becomes more likely.

To view the current power usage on a USB hub—even an internal one that just manages a computer's physical USB ports—open the Device Manager Properties page for a USB hub. On that page, select the Power tab to see a list of the devices connected to the hub and the power required to operate each device (Figure 3-25).



The hub is self-powered.

Total power available: 500 mA per port

Description	Power Required
USB Mass Storage Device	200 mA
5 port(s) available	0 mA

To update the list, click Refresh.

FIGURE 3-25 Hub showing a device consuming 200 mA of power

Lesson summary

- There are several versions of USB, each with its own speed limit.
- Device Manager is used to enable and disable devices.
- There are two kinds of USB hubs: bus-powered and self-powered.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. How fast is USB 2.0?

   A. 400 Mbps

   B. 480 Mbps

   C. 12 Mbps

   D. 5 Gbps

2. Which is more important: bandwidth or power usage on USB?

   A. Bandwidth.

   B. Power.

   C. They are equally important.

   D. Neither is important.

Lesson 3: Managing enterprise hardware policies

Enterprises have stricter requirements with regard to hardware than do home computers. In the enterprise, the ramifications are far greater if information is stolen or if malware infects the organization.

After this lesson, you will be able to:

- Understand how you can prevent the installation of all removable devices.
- Describe which policies allow or prevent device installation on a granular basis.
- Describe the difference between device ID strings and device classes.
- Identify the ID string and class for a hardware device.

Estimated lesson time: 40 minutes

Managing enterprise hardware installation policies

Administrators can create organizational policies that define how devices are managed by using Group Policy. You can disable the installation of removable devices completely, or you can take a more surgical approach by allowing or preventing the installation of removable devices.

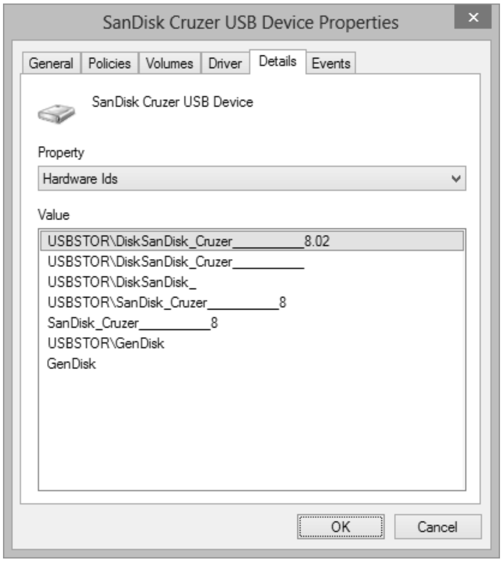
Before undertaking this effort, make sure you understand the two ways by which you can choose devices to allow or prevent such installations:

- **Device identification strings** This is the most granular way to allow or prevent the installation of hardware devices. By using this method, you can identify specific devices to include in the policy.
- **Device setup classes** By using device setup classes, you take a group-based approach to allow or prevent hardware devices from being installed. For example, you could prevent the installation of any device that's a scanner.

Identifying hardware strings and classes

To identify the hardware string and class for a hardware device:

1. Plug the device into a Windows-based computer.
2. Open Device Manager.
3. Open the Properties page for the newly installed device.
4. Navigate to the device's Details page.
    - Select the Hardware Ids property to view all the hardware IDs associated with the device (Figure 3-26).
    - Select the Compatible Ids property to view the device class for the new device (Figure 3-27).



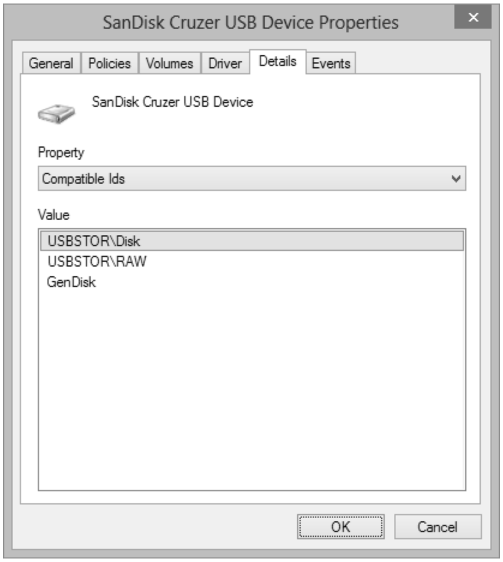
SanDisk Cruzer USB Device

Property: Hardware Ids

Value:

```
USBSTOR\DiskSanDisk_Cruzer__________8.02
USBSTOR\DiskSanDisk_Cruzer__________
USBSTOR\DiskSanDisk_
USBSTOR\SanDisk_Cruzer__________8
SanDisk_Cruzer__________8
USBSTOR\GenDisk
GenDisk
```

FIGURE 3-26 Hardware IDs for a USB thumb drive



SanDisk Cruzer USB Device

Property: Compatible Ids

Value:

```
USBSTOR\Disk
USBSTOR\RAW
GenDisk
```

FIGURE 3-27 Compatible IDs for a USB thumb drive

Note that there are multiple options for both hardware ID and class ID. For the hardware ID, the options give you a way to be somewhat granular in how you handle devices. For example, you could choose to prevent or allow just SanDisk devices or prevent or allow just the specific device model.

REAL WORLD **COPY AND PASTE THE HARDWARE ID**

To save a lot of trouble, copy and paste the hardware IDs rather than trying to type them and match the number of underscore characters. You will minimize errors this way.

Disabling installation of removable devices

High-security organizations do not generally allow the use of any removable devices on a system. To do so would enable an insider to just connect a USB thumb drive and steal corporate assets or other secrets. By using Group Policy, it's possible to disable the installation of removable devices completely. The Group Policy described in the following list will, when set, enable you to disable the installation of removable devices on as many computers in your organization as you like:

- **Policy name** Prevent Installation Of Removable Devices.
- **Policy path** Windows Settings, Administrative Templates, System, Device Installation, Device Installation Restrictions.
- **Policy description** This policy setting enables you to prevent Windows from installing removable devices. A device is considered removable when its driver indicates that the device is removable. For example, a USB device is reported to be removable by the drivers for the USB hub to which the device is connected. This policy setting takes precedence over any other policy setting that allows Windows to install a device.
- **Enabled** If you enable this policy setting, it prevents Windows from installing removable devices, and the drivers for existing removable devices cannot be updated. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of removable devices from a remote desktop client to the remote desktop server.
- **Disabled or not configured** If you disable or do not configure this policy setting, Windows can install and update device drivers for removable devices as allowed or prevented by other policy settings.

Managing installation of specific devices based on device ID or group

The ability to prevent the installation of removable devices is nice, but it is a heavy-handed approach to the problem. Other policies are available by which you can be a bit more granular in how you handle allowed and disallowed devices.

For these policies, you need to know the class of the device.

RESTRICTING DEVICE INSTALLATION BASED ON CLASS

The following Group Policy enables you to specify device classes that are not allowed to be installed in the organization:

- **Policy name** Prevent installation of devices using drivers that match these devices' setup classes.

- **Policy path** Windows Settings, Administrative Templates, System, Device Installation, Device Installation Restrictions.
- **Policy description** This policy setting enables you to specify a list of device setup class globally unique identifiers (GUIDs) for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.
- **Enabled** If you enable this policy setting, Windows is prevented from installing or updating device drivers whose device setup class GUIDs appear in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.
- **Disabled or not configured** If you disable or do not configure this policy setting, Windows can install and update devices as allowed or prevented by other policy settings.

ALLOWING DEVICE INSTALLATION BASED ON CLASS

The following Group Policy enables you to specify device classes that are allowed to be installed in the organization. Use this policy only when you also configure the Prevent Installation Of Devices Not Described By Other Policy Settings policy setting. This policy overrides the hardware installation restrictions for any device classes you list.

- **Policy name** Prevent installation of devices using drivers that match these devices' setup classes.
- **Policy path** Windows Settings, Administrative Templates, System, Device Installation, Device Installation Restrictions.
- **Policy description** This policy setting enables you to specify a list of device setup class GUIDs for device drivers that Windows is allowed to install. Use this policy setting only when the Prevent Installation Of Devices Not Described By Other Policy Settings policy setting is enabled. Other policy settings that prevent device installation take precedence over this one.
- **Enabled** If you enable this policy setting, Windows is allowed to install or update device drivers whose device setup class GUIDs appear in the list you create unless another policy setting specifically prevents installation. (Examples are the Prevent Installation Of Devices That Match These Device IDs policy setting, the Prevent Installation Of Devices For These Device Classes policy setting, and the Prevent Installation Of Removable Devices policy setting). If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.
- **Disabled or not configured** If you disable or do not configure this policy setting, and no other policy setting describes the device, the Prevent Installation Of Devices Not Described By Other Policy Settings policy setting determines whether the device can be installed.

RESTRICTING DEVICE INSTALLATION BASED ON HARDWARE ID

The following Group Policy enables you to specify device IDs that are not allowed to be installed in the organization. You need to specify hardware IDs when enabling this policy.

- **Policy name** Prevent installation of devices that use any of these device IDs.
- **Policy path** Windows Settings, Administrative Templates, System, Device Installation, Device Installation Restrictions.
- **Policy description** This policy setting enables you to specify a list of plug-and-play hardware IDs and compatible IDs for devices that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.
- **Enabled** If you enable this policy setting, Windows is prevented from installing a device whose hardware ID or compatible ID appears in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.
- **Disabled or not configured** If you disable or do not configure this policy setting, devices can be installed and updated as allowed or prevented by other policy settings.

ALLOWING DEVICE INSTALLATION BASED ON HARDWARE ID

The following Group Policy enables you to specify device IDs that are allowed to be installed in the organization. You need to specify hardware IDs when enabling this policy.

- **Policy name** Allow installation of devices that use any of these device IDs.
- **Policy path** Windows Settings, Administrative Templates, System, Device Installation, Device Installation Restrictions.
- **Policy description** This policy setting enables you to specify a list of plug-and-play hardware IDs and compatible IDs for devices that Windows is allowed to install. Use this policy setting only when the Prevent Installation Of Devices Not Described By Other Policy Settings policy setting is enabled. Other policy settings that prevent device installation take precedence over this one.
- **Enabled** If you enable this policy setting, Windows is allowed to install or update any device whose plug-and-play hardware ID or compatible ID appears in the list you create unless another policy setting specifically prevents that installation. (Examples are the Prevent Installation Of Devices That Match Any Of These Device IDs policy setting, the Prevent Installation Of Devices For These Device Classes policy setting, and the Prevent Installation Of Removable Devices policy setting). If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.
- **Disabled or not configured** If you disable or do not configure this policy setting, and no other policy setting describes the device, the Prevent Installation Of Devices Not Described By Other Policy Settings policy setting determines whether the device can be installed.

Creating an administrative override for device installation

As an administrator, it might be necessary to install a device that is generally restricted in the organization. To accomplish this goal, use the following policy settings:

- **Policy name** Allow administrators to override Device Installation Restriction policies.
- **Policy path** Windows Settings, Administrative Templates, System, Device Installation, Device Installation Restrictions.
- **Policy description** This policy setting enables you to determine whether members of the Administrators group can install and update the drivers for any device regardless of other policy settings.
- **Enabled** If you enable this policy setting, members of the Administrators group can use the Add Hardware Wizard or the Update Driver Wizard to install and update the drivers for any device. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.
- **Disabled or not configured** If you disable or do not configure this policy setting, members of the Administrators group are subject to all policy settings that restrict device installation.

MORE INFO **CONTROLLING DEVICE INSTALLATION BY USING GROUP POLICY**

Microsoft has created a resource entitled *Step-By-Step Guide to Controlling Device Installation Using Group Policy*, which provides in-depth information about how to use the various Group Policy objects to control hardware installation in an organization better. It's an invaluable resource for any administrator who wants to implement granular controls over hardware devices; find it at *http://msdn.microsoft.com/en-us/library/bb530324.aspx*.

Lesson summary

- Hardware strings enable you to be as inclusive or as granular as you like when you must allow or prevent the installation of hardware devices.
- By using the Allow Administrators To Override Device Installation Restriction Policies policy, you can implement restrictive policies in the organization but still leave room for special cases.
- Device setup classes are used to take a device group–based approach to hardware management.
- When you enable the Prevent Installation Of Devices Not Described By Other Policy Settings policy, you should create policies that enable specific devices to override the restriction policies.
- Group Policy provides you with an easy way to create hardware installation policies across the organization.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which hardware strings could be used to restrict the installation of a hardware device with ID USBSTOR\DiskSanDisk_Cruzer__________8.02? (Choose all that apply.)

   A. USBSTOR\DiskSanDisk_Cruzer__________8.02

   B. USBSTOR\DiskSanDisk_Cruzer__________

   C. USBSTOR\DiskSanDisk_

   D. USBSTOR\SanDisk_Cruzer__________8

2. Which method will encompass and restrict the greatest number of devices?

   A. Hardware ID

   B. Class ID

   C. Device Name

   D. Device SID

3. How do you allow an administrator to install hardware even when Group Policy forbids it?

   A. Enable the Allow Administrators To Override Device Installation Restriction Group Policy.

   B. Add the Administrators group to the No Hardware Restrictions group.

   C. Add users to the local Administrators group on their PCs.

   D. Enable Admin Mode in Device Manager.

Practice exercises

In these practice exercises, you navigate from the Windows 8 Start screen to find hardware IDs and create Group Policy to allow or prevent the installation of devices.

Exercise 1: Locate hardware ID for a USB thumb drive

In this exercise, you identify the specific hardware ID for a USB thumb drive. You probably have one of these devices lying around somewhere.

1. Open Device Manager.
2. Find your device.
3. Using the device properties, find the hardware ID.

Exercise 2: Create Group Policy to prevent the installation of hardware devices

In this exercise, you create Group Policy that prevents the installation of removable devices. To complete this exercise, your Windows 8 system must be joined to a Microsoft Windows Server domain.

1. Use the Group Policy Editor on the computer running Windows Server.
2. Configure the appropriate Group Policy and test it.

Suggested practice exercises

The following additional practices are designed to give you more opportunities to practice what you've learned and to help you successfully master the lessons presented in this chapter.

- **Exercise 1** Practice configuring and applying Group Policy to see how each policy works.
- **Exercise 2** Use Driver Verifier and learn to interpret its output.
- **Exercise 3** Add drivers to the Driver Store.

Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct answer: C**
    - **A. Incorrect:** Device Manager is a read/write tool used to manage devices and drivers.
    - **B. Incorrect:** Driver Verifier locates deep-rooted driver issues.
    - **C. Correct:** System Info displays general information about hardware and software configured on a computer. Information displayed is read-only.
    - **D. Incorrect:** Computer Management is a general-purpose tool used to manage the system.
2. **Correct answer: B**
    - **A. Incorrect:** Driver Verifier checks the installation of device drivers; it does not display hidden devices.
    - **B. Correct:** The Device Manager View menu can show or hide hidden devices.
    - **C. Incorrect:** Selecting a device category will expand and collapse devices within that category, but doing so does not change the hidden status of a device.
    - **D. Incorrect:** There is no Hidden Devices node in System Info.
3. **Correct answer: A**
    - **A. Correct:** Driver Verifier locates driver issues.
    - **B. Incorrect:** Drivers can be installed by using this method.
    - **C. Incorrect:** Drivers can be installed by using this method.
    - **D. Incorrect:** Drivers can be installed by using this method.

Lesson 2

1. **Correct answer: B**
    - **A. Incorrect:** FireWire runs at 400 Mbps, which is slower than USB 2.0.
    - **B. Correct:** USB 2.0 has bandwidth typically around 480 Mbps.
    - **C. Incorrect:** USB 1.1 maintained speeds of around 12 Mbps.
    - **D. Incorrect:** USB 3.0 is rated at around 5 Gbps.

2. **Correct answer: C**
   - **A.** **Incorrect:** Bandwidth issues can cause problems ensuring that a USB device has enough power to function correctly.
   - **B.** **Incorrect:** Improperly powered USB devices can affect bandwidth and performance of the device.
   - **C.** **Correct** Power and bandwidth are equally important in determining USB device performance because underpowered devices will suffer bandwidth performance issues.
   - **D.** **Incorrect:** USB has two components that are typically watched, bandwidth and power, and both are equally important in determining device performance.

Lesson 3

1. **Correct answers: A, B, C, and D**
   - **A.** **Correct:** Installation of the specific device with version 8.02 will be prevented.
   - **B.** **Correct:** No DiskSanDisk_Cruzer device can be installed, which includes the device in question.
   - **C.** **Correct:** No SanDisk-based device can be installed.
   - **D.** **Correct:** No DiskSanDisk_Cruzer version 8 device can be installed, which includes the device in question.
2. **Correct answer: B**
   - **A.** **Incorrect:** The device ID would include only this specific device.
   - **B.** **Correct**: The class ID for a set of devices would include any devices of the same class.
   - **C.** **Incorrect:** The device name would include only devices with the same name, much like device ID covers only a specific device.
   - **D.** **Incorrect:** Hardware devices are not assigned a SID; these are reserved for logical objects such as user accounts or computer accounts.
3. **Correct answer: A**
   - **A.** **Correct:** Enable the Group Policy options to allow an override.
   - **B.** **Incorrect:** There is no group called No Hardware Restrictions for use with this feature.
   - **C.** **Incorrect:** Adding accounts to the local Administrators group will not specifically allow this action; Group Policy options must be configured so that domain administrators can override settings.
   - **D.** **Incorrect:** The Device Manager snap-in does not have an admin mode specific to computer hardware; the MMC console has an author mode, but that is used to manage the console.

Index

Numbers and Symbols

802.11 standard, 281

A

accelerators, 170
access control
  for hardware, 132–133
  installed applications, 132–133
  for native applications, 131–133
  for Remote Desktop tool, 300–301
  for Windows Store apps, 131
access control entries (ACEs), 392
access control lists (ACLs), 392
ACEs (access control entries), 392
ACLs (access control lists), 392
ACT (Application Compatibility Toolkit), 122
Active command (DiskPart), 387
Active Directory Administrator's Pocket Consultant (Stanek), 426
Active Directory domains
  about, 43
  additional information, 426
  assigning user rights, 438–439
  authenticating users, 420–421
  domain-based authentication, 422
  joining, 44
  managing IE settings, 153–155
Active Time metric, 505
ActiveX Control snap-in (MMC), 329
ActiveX controls
  about, 166
  controlling ActiveX opt-in, 166–168
  managing behavior, 168–169
  running using Group Policy, 172–173
Add-AppxPackage cmdlet, 138
Add-AppxProvisionedPackage cmdlet, 138
Add command (DiskPart), 387
Add Counters window, 518–519
add-ons (plug-ins)
  about, 13, 165
  challenges using, 165
  disabling, 171
  enabling, 171
  managing accelerators, 170
  managing ActiveX controls, 166–169
  managing search providers, 170
  managing toolbars and extensions, 169–170
  managing tracking protection, 170
  managing with Group Policy, 172–175
  preventing installation of, 173
  specifying approved, 174–175
  starting IE without, 171–172
Address Space Layout Randomization (ASLR), 157
ADK (Assessment and Deployment Kit), 61
administering authentication
  about, 419–420
  biometric authentication, 427–428
  configuring Microsoft accounts, 430–431
  domain-based authentication, 422
  for file systems, 392

IPsec settings, 268
Kerberos authentication, 422–423, 449
lesson summary, 436
logging on with picture passwords, 432–435
managing credentials, 428–430
with PIN, 435
practice exercises, 459–460
process overview, 420–421
public key, 444
Remote Desktop tool, 307
review questions and answers, 436–437, 461
security account manager database authentication, 422
smart card authentication, 425–427
user name and password-based authentication, 422–424
using certificates for, 318, 420
VPNs, 318–319
Windows Firewall with Advanced Security, 268, 273
administering authorization
about, 419, 437
assigning user rights, 437–443
Local Security Policy console, 443–452
managing certificates, 455–457
“run as” considerations, 454–455
running tasks as administrator, 452–454
user rights, 437–438
user rights versus permissions, 438
working in groups, 438
administering networking
configuring networking, 223–247
lesson summaries, 246, 255
practice exercises, 256–257
review questions and answers, 246–247, 255–256, 258–259
troubleshooting networking, 247–256, 310–314
administrative tools, adding tiles for, 7–8
administrator account
changing name of, 444
local security options, 444, 451
password policies, 283
running tasks as, 452–454
User State Migration Tool, 57
WORKGROUP work group and, 44
Administrators group, 392
Advanced Boot Options screen, 535
Advanced Encryption Standard (AES), 281, 450
Advanced Security Settings dialog box
Auditing tab, 400–401
Effective Access tab, 360–361, 398–399
Permissions tab, 356–359, 395
Advanced Sharing dialog box, 351
Advanced Sharing Settings dialog box, 231–232, 347–348
AES (Advanced Encryption Standard), 281, 450
airplane mode feature, 481
All Apps option (apps), 5
Allow permissions, 355
APIPA (Automatic Private IP Addressing), 232–233
APIs (application programming interfaces)
User Rights elements, 440, 443
WinRT, 4
App-V technology, 122–123
AppContainer mechanism, 160
Application Compatibility Toolkit (ACT), 122
application programming interfaces (APIs)
User Rights elements, 440, 443
WinRT, 4
Application Virtualization, 122–123
applications
adding from Windows Store, 14–17
changing affinity settings, 509–510
closing, 11
differences between apps and, 4
managing traditional desktop, 119–128
switching between, 10–11
Task Manager statistics, 506–507
testing for compatibility, 122–125, 184
testing for Windows To Go usage, 48

Windows 8 native, 129–141
AppLocker feature
about, 133
controlling applications, 133–137
defining rules, 133–134
enforcing rules, 134–137
apps
about, 3–4
configuring Windows Firewall to allow, 263–264
differences between applications and, 4
installing, 15
installing on multiple devices, 128
inventorying, 139–140
management options for, 5–6
removing, 139–140
removing from Windows Firewall configuration, 264
sharing options, 9
sideloading, 137–139
Task Manager statistics, 506–507
archives, saving events to, 517
Armstrong, Ben, 188
ASLR (Address Space Layout Randomization), 157
Assessment and Deployment Kit (ADK), 61
Assign command (DiskPart), 387
ATM technology, 425
Attach command (DiskPart), 387
Attributes command (DiskPart), 387
auditing
access to securable objects, 400–402
user rights assignments and, 439
Authenticated Users group, 392
authentication
about, 419–420
biometric, 427–428
configuring Microsoft accounts, 430–431
domain-based, 422
for file systems, 392
IPsec settings, 268
Kerberos, 422–423, 449
lesson summary, 436
logging on with picture passwords, 432–435
managing credentials, 428–430
with PIN, 435
practice exercises, 459–460
process overview, 420–421
public key, 444
Remote Desktop tool, 307
review questions and answers, 436–437, 461
security account manager database, 422
smart card, 425–427
user name and password-based, 422–424
using certificates for, 318, 420
VPNs, 318–319
Windows Firewall with Advanced Security, 268, 273
authorization
about, 419, 437
assigning user rights, 437–443
Local Security Policy console, 443–452
managing certificates, 455–457
"run as" considerations, 454–455
running tasks as administrator, 452–454
user rights, 437–438
user rights versus permissions, 438
working in groups, 438
Authorization Manager snap-in (MMC), 329
Automatic Maintenance window, 492–493
Automatic Private IP Addressing (APIPA), 232–233
Automount command (DiskPart), 387
Average Response Time metric, 505

B

backup and restoration
backing up Windows 8, 528–530
creating additional images, 530
creating system repair or recovery disc, 549–550

- disabling restart after failure, 552
- MSConfig utility, 544–546
- protecting files and data with File History, 530–535
- recovering from bad driver installation, 546–547
- Refresh method, 539–540
- Reset method, 539, 541–543
- restoring an entire computer, 535–536
- Task Manager Startup tab, 546
- using System Restore, 536–539
- Windows Recovery Environment, 550–552

bandwidth considerations
- for Remote Desktop, 306
- reporting device consumption, 106
- Windows Update and, 499

basic disks, 373, 377

basic input/output system (BIOS), 22–23, 185, 284–285

Bcdboot.exe command, 48

Bing toolbar, 169

biometric authentication, 427–428

BIOS (basic input/output system), 22–23, 185, 284–285

BitLocker Drive Encryption
- about, 404, 444, 464
- configuring policies, 464–466
- enabling without TPM, 468–470
- managing at command line, 466–468
- on removable media, 404, 466, 470–471
- Windows editions and, 28
- Windows To Go and, 21, 45–46

BitLocker To Go, 404, 466, 470–471

boot disks, creating, 50

Break command (DiskPart), 387

bring your own device (BYOD) initiatives, 21

broadcast addresses, 236–237

browser extensions, 170

browser helper objects, 169–170

browsers. *See specific browsers*

bus-powered USB hubs, 105

BYOD (bring your own device) initiatives, 21

C

CA (certificate authority), 426, 455–457

caching, offline, 533

Calendar application, 431

capabilities and feature in Windows 8
- about, 1–2, 12–23
- lesson summary, 24
- navigating Windows 8 user interface, 2–12
- in networking, 224–225
- practice exercises, 33
- review questions and answers, 24–25, 34

Capacity metric, 505

certificate authority (CA), 426, 455–457

certificate-based credentials, 429

Certificate Export Wizard, 403

Certificate Manager, 456–457

certificate stores, 328, 456

certificates
- for authentication, 318, 420
- credentials and, 429
- EFS, 530
- local security options, 451
- managing, 329, 402–403, 455–457
- Secure Boot feature validating, 284
- sign-in process and, 426
- smart cards and, 425–427
- SSL, 245, 455
- Unified Communications, 455

Certificates snap-in (MMC), 329, 402

Challenge Handshake Authentication Protocol (CHAP), 319

Change Settings window, 491–492

CHAP (Challenge Handshake Authentication Protocol), 319

charms, 7–10

Chat feature (Remote Assistance), 296–297
chkdsk utility, 383–386
Chrome browser, 149
class ID
  about, 108–110
  installing based on, 110–113
Clean command (DiskPart), 387
Clear Selection option (apps), 5
cloud computing
  about, 19–21
  authentication and, 423
  Microsoft accounts and, 19, 423, 431
cmdlets. *See specific cmdlets*
command line
  getting help for commands, 387
  managing BitLocker at, 466–468
  remote management tools, 323–326
  running USMT from, 56–60
  setting up Windows To Go from, 46–48
  starting IE without add-ons, 172
  troubleshooting tools, 254–255
  viewing network settings, 250–251
Compact command (DiskPart), 387
Component Services snap-in (MMC), 329
computer accounts
  assigning certificates, 457
  authorizing connections, 274
  local security options, 445–446
Computer Management snap-in (MMC), 329
Computer Name/Domain Changes dialog box, 44
Control Panel
  accessing, 132, 228–229, 276
  accessing Network and Sharing Center, 228, 276, 310, 344–345
  accessing user rights, 439
  accessing Windows Update settings, 488–490
  adding devices, 132–133
  assigning user rights, 437
  backing up data, 528
  backing up personal settings, 531
  configuring biometric sign-ins, 428
  configuring offline file synchronization, 473
  configuring printing permissions, 366
  configuring shared printers, 364
  configuring System Restore, 537
  connecting to VPNs, 315
  creating storage spaces, 410–412
  creating system images, 530
  creating system repair or recovery disc, 549
  Devices section, 132
  enabling/disabling IE add-ons, 171–172
  enabling Enhanced Protected Mode in IE, 158, 163
  enabling Remote Desktop access, 300
  managing credentials, 428
  opening BitLocker Drive Encryption, 404
  opening Device Manager, 82–83
  opening Networks taskbar, 242
  opening Windows To Go, 45, 75
  recovering from bad driver installation, 547
  resetting IE as default browser, 149
  restoring data, 533
  rolling back updates, 497
  starting Local Computer Policy snap-in, 423
  System page, 30–31
controlling access
  for hardware, 132–133
  installed applications, 132–133
  for native applications, 131–133
  for Remote Desktop tool, 300–301
  for Windows Store apps, 131
Convert command (DiskPart), 387
CoreInfo tool, 18
counters, performance, 518–519
CPU metric, 503
CPU Time metric, 506
Create A Storage Space window, 410–411
Create A System Image Wizard, 530
Create command (DiskPart), 387
Create Packaged App Rules Wizard, 136

Credential Manager
- accessing, 428
- managing, 429–430
- User Rights elements, 439

credentials
- authentication and, 420–421
- managing, 428–430
- PINs and, 435
- types of, 429–430

cumulative application, 398

D

DACLs (Discretionary Access Control Lists), 392–394, 450

data management, Hyper-V and, 184–185

Davies, Joseph, 236

decryption. *See* encryption

default gateways
- about, 234–235
- adding second, 240–241

Default Media Streaming Settings page, 279

default programs, configuring, 126

Delete command (DiskPart), 387

denial-of-service attacks, 282

Deny permissions, 355, 394, 398–399

desktop applications and interface
- about, 119
- accessing Windows Update, 489
- controlling program settings for, 123–126
- Internet Explorer 10 and, 145–153
- lesson summary, 126–127
- managing compatibility with ACT, 122
- managing compatibility with App-V, 122–123
- review questions and answers, 127, 143
- Windows Installer and, 120–122

Detach command (DiskPart), 388

Detail command (DiskPart), 387

device drivers
- about, 79
- adding to driver store, 102–103
- Device Manager, 81–93
- Driver Verifier utility, 95–101
- installation methods for, 80
- managing, 88–91
- pre-staging, 80
- recovering from bad installation, 546–547
- rolling back, 91
- System Information utility, 93–95
- types of, 81
- updating, 91
- viewing information, 83–88

device identification strings, 108–110

Device Manager snap-in (MMC)
- about, 81, 329
- Advanced tab, 85–86
- Details tab, 86
- displaying hidden devices, 92–93
- Driver tab, 86, 89–91
- enabling and disabling devices, 104–105
- Events tab, 86–87
- General tab, 84–85
- managing drivers, 88–91
- opening, 82–83
- Properties page, 106
- Resources tab, 87–88
- viewing device and driver information, 83–88

device setup classes, 108–110

Devices charm, 10

devmgmt.msc command, 83

DHCP (Dynamic Host Configuration Protocol)
- configuring IP settings, 232–234
- configuring name resolution, 238

diagnostics, system, 520–521

dial-up connections, 321

digital signatures, 81, 455–456

DirectAccess tool, 254

Disable-BitLocker cmdlet, 468

disabling
- add-ons, 171–172
- devices, 104–105
- hardware devices, 104–105
- IE Protected Mode, 161
- installation of removable media, 110
- local accounts, 60
- Windows Store app, 131

Discretionary Access Control Lists (DACLs), 392–394, 450

Disk Cleanup dialog box, 378–380

Disk Cleanup utility
- about, 377
- performing maintenance, 378–380

Disk Defragmenter tool, 377

disk management
- about, 371–373
- BitLocker policy settings and, 464–466
- chkdsk utility, 383–386
- creating boot disks, 50
- Disk Cleanup utility, 377–380
- Disk Defragmenter tool, 377
- disk quotas in file systems, 405–408
- DiskPart utility, 66–69, 386–390
- Hyper-V requirements, 17, 193, 200, 208–210
- lesson summary, 390
- Microsoft Drive Optimizer tool, 380–383
- review questions and answers, 390–391, 416
- Task Manager statistics, 503, 505
- transferring files via external hard disks, 55–56
- Windows 8 requirements, 29

Disk Management snap-in (MMC)
- about, 329, 372–373
- actions available, 375–377
- disk types supported, 373–374
- DiskPart utility and, 388
- opening, 372
- partition types supported, 374
- volume types supported, 374–375

Disk metric, 503

disk pools
- about, 410
- creating storage spaces, 410–412

disk quotas in file systems, 405–408

DiskPart utility
- about, 386–390
- Active command, 387
- Add command, 387
- Assign command, 387
- Attach command, 387
- Attributes command, 387
- Automount command, 387
- Break command, 387
- Clean command, 387
- commands supported, 387–388
- Compact command, 387
- Convert command, 387
- Create command, 387
- creating VHDs from existing installations, 66–69
- Delete command, 387
- Detach command, 388
- Detail command, 387
- Disk Management console and, 388
- Exit command, 388
- Expand command, 388
- Extend command, 388
- Filesystems command, 388
- Format command, 388
- GPT command, 388
- Help command, 388
- Import command, 388
- Inactive command, 388
- List command, 388
- Merge command, 388
- Offline command, 388
- Online command, 388
- Recover command, 388
- Rem command, 388
- Remove command, 388

Repair command, 388
Rescan command, 388
Retain command, 388
SAN command, 388
Select command, 388
SetID command, 388
Shrink command, 388–389
UniqueID command, 388
DISM utility, 47, 138, 140
distinguished name (DN), 455
DN (distinguished name), 455
DNS (Domain Name Server)
configuring IP settings, 235
configuring name resolution, 238–239
documentation, importance of, 322, 397, 469
domain-based authentication, 422
Domain Name Server (DNS)
configuring IP settings, 235
configuring name resolution, 238–239
domain profiles, 265
dotted quad notation, 235
double-tap action, 3
Drive Optimizer application, 380–383
Driver File Details page, 90
Driver Properties dialog box, 378
Driver Verifier utility, 95–101
drivers
about, 79
adding to driver store, 102–103
Device Manager, 81–93
Driver Verifier utility, 95–101
installation methods for, 80
managing, 88–91
pre-staging, 80
recovering from bad installation, 546–547
rolling back, 91
System Information utility, 93–95
types of, 81
updating, 91
viewing information, 83–88
dual TCP/IP stack, 237–238
dynamic disks, 373, 377
Dynamic Host Configuration Protocol (DHCP)
configuring IP settings, 232–234
configuring name resolution, 238
dynamic memory, 198

E

EAP (Extensible Authentication Protocol), 281, 318
Easy Connect feature, 296
Easy Transfer cable, 54
Edge UI
about, 8–9
opening, 10
EFS (Encrypting File System)
about, 402–404, 464
certificate support, 530
ScanState options, 58
EFS key, 403–404
802.11 standard, 281
Enable-BitLocker cmdlet, 468
enabling
add-ons, 171
BitLocker Drive Encryption without TPM, 468–470
devices, 104–105
folder sharing for profiles, 346–347
groups on local computer, 329
hardware devices, 104–105
Hyper-V, 184–186
IE Enhanced Protected Mode, 158–159, 163
local accounts, 60
Remote Desktop access, 300
System Restore, 539
Encrypting File System (EFS)
about, 402–404, 464
certificate support, 530
ScanState options, 58

encryption
- BitLocker Drive Encryption, 21, 28, 45–46, 404, 444, 464–471
- configuring policy settings for offline files, 471, 475
- Encrypting File System, 58, 402–404, 464, 530
- file sharing and, 278, 348
- inbound rules and, 270
- IPsec settings, 268
- local security options, 445–447, 449–450
- Remote Assistance and, 297
- ScanState options, 58–59
- Server Message Block, 224
- VPNs and, 318–319
- Windows Remote Shell, 326
- Windows RT, 28
- wireless networks, 246, 281, 283

End User License Agreement (EULA), 38, 50

enhanced memory protection (IE), 157

Enhanced Protected Mode (IE)
- enabling, 158–159, 163
- running using Group Policy, 172–173

enterprise hardware policies, managing, 107–114

Enterprise PKI, 426

EULA (End User License Agreement), 38, 50

evaluating Windows 8
- differences between editions, 25–32
- lesson summaries, 24, 31
- new features and capabilities, 1–25
- practice exercises, 32–33
- review questions and answers, 24–25, 31–32, 34–35

event logs
- about, 513–514
- configuring, 514–515
- filtering, 515–517
- saving events to archive, 517

Event Viewer snap-in (MMC)
- about, 329
- accessing, 513–514
- Actions pane, 514, 516
- configuring event logs, 514–515
- filtering events, 515–517
- saving events to archives, 517

Exchange Management Console, 305

executable rules, 133

Exit command (DiskPart), 388

Expand command (DiskPart), 388

Export Successful dialog box, 403

Extend command (DiskPart), 388

Extend Volume Wizard, 376

extended partition type, 374

Extensible Authentication Protocol (EAP), 281, 318

extensions, browser, 170

external hard disks, transferring files via, 55–56

external virtual switches, 199, 210–211

F

features and capabilities in Windows 8
- about, 1–2, 12–23
- lesson summary, 24
- navigating Windows 8 user interface, 2–12
- in networking, 224–225
- practice exercises, 33
- review questions and answers, 24–25, 34

File and Printer Sharing mechanism
- about, 232
- for network discovery profiles, 276–277
- for private networks, 347
- VPN support, 320

file associations, configuring, 126

File History feature
- about, 530–531
- excluding items from, 532–533
- restoring backups, 533–535

File Recovery Wizard (Windows 7), 529

file sharing
- about, 343, 346–352

configuring Network and Sharing Center, 344–345
encryption and, 278, 348
File and Printer Sharing mechanism, 232, 276–277, 320, 347
NTFS permissions, 352–362
file systems
about, 391
auditing access to securable objects, 400–402
BitLocker support, 404
chkdsk utility scans, 385
Encrypting File System, 402–404
inheritance and cumulative effectiveness, 397–399
lesson summary, 408
review questions and answers, 408–409, 417
security within, 391–397
share-level permissions, 400
taking ownership, 399
working with quotas, 405–408
file transfers
migrating user data, 60–63
via User State Migration Tool, 56–60
via Windows Easy Transfer, 53–56
files, offline, 471–476
Filesystems command (DiskPart), 388
filtering event logs, 515–517
fingerprint-reading devices, 427
Firefox browser, 149
firewall profiles, 265–267
firewalls
about, 261–262
configuring rules, 269–274
as Windows Action Center source, 511
Windows Firewall options, 262–264
Windows Firewall with Advanced Security options, 264–274
fixed-size VHD files, 67
Flash plug-in, 13, 166
folder sharing
about, 343, 346–352
configuring Network and Sharing Center, 344–345
network discovery profiles and, 277
NTFS permissions, 352–362
troubleshooting, 253, 313
Folder snap-in (MMC), 329
Forced Address Space Layout Randomization (ASLR), 157
Format command (DiskPart), 388
Formatted metric, 505
Full Control permission
about, 353
managing file system objects, 394, 396
share-level permissions and, 400
shared folders, 352, 362

G

Gage, John Burdette, 223
gateways, default
about, 234–235
adding second, 240–241
Get-AppxPackageManifest cmdlet, 139
Get-Process cmdlet, 327–328
gpedit.msc (Local Group Policy Editor)
BitLocker on removable media, 471
BitLocker without TPM, 469
configuring settings, 466, 478
disabling Windows Store app, 131
enforcing rules, 135, 137
GPO (Group Policy Object), 469–470
GPT command (DiskPart), 388
GPT (GUID Partition Table), 373–374, 377
gpupdate command, 131, 137
Group Policy
additional information, 478
configuring location-based services, 481

controlling access to Windows Store apps, 131
controlling IE Start screen tile behavior, 155
disabling installation of removable devices, 110
installation based on device ID or group, 110–113
managing IE add-ons with, 172–175
managing IE settings, 153–155
managing link behavior, 154
preventing installation of add-ons, 173
Remote Assistance settings, 295
sideloading apps, 137
specifying approved add-ons, 174–175
Windows Installer and, 120–121
Windows Update and, 499–500
Group Policy Management Console, 153–154
Group Policy Object Editor snap-in (MMC), 329
Group Policy Object (GPO), 469–470
groups
about, 396
adding, 393
default, 392
enabling on local computer, 329
permissions and, 353, 356–358, 394, 397–400
security settings, 443, 445
taking ownership of resources, 361–362
user rights and, 437–443
verifying existing, 394
guest enlightenment, 187
guest profiles, 277, 348
GUID Partition Table (GPT), 373–374, 377

H

hardware and device drivers
lesson summaries, 103, 107, 113
managing access to, 132–133
managing drivers, 79–104
managing enterprise hardware policies, 107–114, 117
managing hardware devices, 104–106
monitoring USB devices, 105–106
practice exercises, 114–115
recovering from bad installation, 546–547
review questions and answers, 103–104, 107, 114, 116–117
troubleshooting, 89–92, 95, 104, 367
verifying software for, 426
hardware ID
about, 108–110
installing based on, 110–113
HBA (host bus adapter), 210
HEASLR (High Entropy Address Space Layout Randomization), 157
Help command (DiskPart), 388
help for commands, 387
Hibernate action, 45
hidden devices, displaying, 92–93
hidden updates, 498–499
High Entropy Address Space Layout Randomization (HEASLR), 157
high integrity level, 160
HomeGroup feature
about, 232, 311
folder sharing and, 348
password considerations, 280
troubleshooting, 253, 313
host bus adapter (HBA), 210
Hotmail service, 430
HTML5
about, 13
sandbox attribute, 157
Hyper-V
about, 17–19, 181–183
configuring, 206, 208–217
core resources, 183
creating virtual machines, 191–192, 195–202
critical elements of, 186–190
data management and licensing, 184–185
enabling, 185–186

hardware requirements, 17, 193, 200, 208–210
lesson summary, 190, 206–207, 216
memory requirements, 18, 185, 193–194, 198
planning virtual machines, 192–194
practice exercises, 217–218
review questions and answers, 191, 207, 217, 219–221
state-changing tasks, 204
storage and networking for virtual machines, 193–194, 204–206, 208–210, 214–216
using virtual machines, 202–206
virtual switch, 210–216
when to use, 183–184

Hyper-V Manager
about, 183, 186
Action menu, 209
creating virtual machines, 195–202

Hyper-V Server
about, 182
creating virtual machines, 195–202

Hyper-V Virtual Switch Manager, 209

hypervisors
about, 17
guest enlightenment and, 187
Type 1, 182
Type 2, 182

I

ICMP (Internet Control Message Protocol), 262, 268–269
IDE controllers, 214–215
identification strings for devices
about, 108–110
installing based on, 110–113
IETF (Internet Engineering Task Force), 236
IFrames (Inline Frames), 157
IKEv2 (Internet Key Exchange Version 2), 318
images, adding sideloaded apps to, 138
Import command (DiskPart), 388
Inactive command (DiskPart), 388
inbound rules, 269–271
indexes, chkdsk utility and, 385
inheritance, permissions and, 356–360, 397–399
initial sign-in screen, 421
Inline Frames (IFrames), 157
installing apps and applications, 15, 128–130
installing drivers, 80
installing native applications, 128–129
installing network adapters, 227–228
installing operating systems in VMs, 203–204
installing Windows 8 on new or formatted systems
configuring accounts, 40–43
joining Active Directory domain, 44
lesson summary, 48
practice exercises, 73–74
review questions and answers, 49, 76
starting installation, 38–39
with Windows To Go, 44–48

installing Windows 8 on startup VHD files
about, 65–66
creating VHD from existing installations, 66–68
creating VHD using DiskPart, 68–69
lesson summary, 72
practice exercises, 74–75
removing VHD installations, 71–72
review questions and answers, 72–73, 78
starting system from VHD, 69–71

Install.wim file, 47–48
Integration Services, 187–188
integrity levels, 160–161
internal virtual switches, 199, 210–212
Internet Connections Troubleshooter, 313–314
Internet Control Message Protocol (ICMP), 262, 268–269
Internet Engineering Task Force (IETF), 236
Internet Explorer 10
about, 12–14

- adding trusted sites, 162
- configuring, 145–156
- configuring browser security settings, 156–164
- controlling Start screen tile behavior, 150–151, 155
- Delete Browsing History setting, 152
- Encoding setting, 153
- Flip Ahead setting, 153
- lesson summary, 155, 164, 175–176
- managing add-ons, 165–176
- managing security settings with Group Policy, 162–163
- Permissions setting, 152
- practice exercises, 176–177
- resetting as default browser, 149
- review questions and answers, 155–156, 164, 176, 178–179
- starting without add-ons, 171–172
- Zoom setting, 153

Internet Explorer Settings page, 151–152
Internet Key Exchange Version 2 (IKEv2), 318
Internet Options page
- configuring default IE experience, 148–149
- controlling IE Start screen tile behavior, 150
- disabling Protected Mode, 161
- enabling Enhanced Protected Mode, 158–159

Internet Protocol Security (IPsec), 267–268
Interrupt Request line (IRQ), 88
inventorying native applications, 139–140
invitations (Remote Assistance), 294–296
IP addresses
- adding second default gateway, 240–241
- changing settings, 237–238
- configuring settings, 232–237
- dotted quad notation, 235
- reserved, 236
- TCP/IP stack and, 237–238
- troubleshooting, 233, 313
- verifying, 234

IP Security Monitor snap-in (MMC), 329
IP Security Policy Management snap-in (MMC), 329
ipconfig command, 250–251, 254
IPsec (Internet Protocol Security), 267–268
IRQ (Interrupt Request line), 88
isatap.localdomain network adapter, 250

J

JBOD (just a bunch of disks), 409

K

Kerberos authentication, 422–423, 449
kernel mode, 442
Key Distribution Center, 422
Kezema, Conan, 426

L

L2TP (Layer 2 Tunneling Protocol), 318
Layer 2 Tunneling Protocol (L2TP), 318
LCP (Link Control Protocol), 317
LDAP (lightweight directory access protocol), 444–445, 449
least privilege principle, 157
licensing
- connection limits and, 351
- ensuring compliance through affinity settings, 509–510
- Hyper-V, 184–185

lightweight directory access protocol (LDAP), 444–445, 449
Link Control Protocol (LCP), 317
Link to Web Address snap-in (MMC), 329
links, managing using Group Policy, 154
Linux operating systems, 187
List command (DiskPart), 388

List Folder Contents permission
  about, 353
  managing file system objects, 394
live tiles, 2
LoadState.exe utility, 57, 59–62
local accounts
  Active Directory domains and, 43–44
  changing back to, 431
  converting to Microsoft account, 430–431
  disabled, 60
  enabled, 60
  local security options, 444, 448
  migrating data, 63
  password considerations, 423
Local Computer Policy snap-in (MMC), 423
Local Group Policy Editor (gpedit.msc)
  BitLocker on removable media, 471
  BitLocker without TPM, 469
  configuring settings, 466, 478
  disabling Windows Store app, 131
  enforcing rules, 135, 137
Local Security Policy console
  assigning user rights, 437–438
  configuring security settings, 443–452
Local Users and Groups snap-in (MMC), 329
location-based services (mobile devices), 152, 481–482
Lock-BitLocker cmdlet, 468
Log Properties page, 514–515
logging on with picture passwords, 432–435
logical unit number (LUN), 216
loopback address, 236
low integrity level, 160
LUN (logical unit number), 216

M

MAC addresses
  about, 208–209, 211
  wireless networking risks, 282
malware, 285–286
Manage Add-Ons window, 171
Manage-bed.exe tool, 466–468
Manage Documents permission, 367
Manage the Printer permission, 367
Master Boot Record (MBR) partitioning style, 373–374
Maximum Password Age setting, 424, 446
Maximum Password Length setting, 424
MBIM (Mobile Broadband Interface Model) standard, 22
MBR (Master Boot Record) partitioning style, 373–374
media
  removable, 53–56, 110, 404, 410, 466, 470–471, 529
  virtualized, 189–190
Media Streaming Options page, 278
medium integrity level, 160
memory considerations
  enhanced memory protection, 157
  Hyper-V, 18, 185, 193–194, 198
  startup memory, 198
  Task Manager statistics, 503–504
  Windows editions and, 29
memory dump files, 378
Memory metric, 503
Merge command (DiskPart), 388
metered connections, 226–227, 244, 492
Metered Network metric, 507
Microsoft accounts
  about, 16
  benefits of, 43
  cloud computing and, 19, 423, 431
  configuring, 430–431
Microsoft CHAP Version 2 (MS-CHAP v2), 319
Microsoft Configuration (MSConfig) utility
  about, 508, 544
  Boot tab, 545

General tab, 545
removing VHD installations, 71
Services tab, 545
Startup tab, 546
Tools tab, 546
Microsoft Exchange servers, 455
Microsoft Knowledge Base articles, 498
Microsoft Management Console (MMC)
about, 328–329
ActiveX Control snap-in, 329
adding snap-ins, 330–332
Authorization Manager snap-in, 329
Certificates snap-in, 329, 402
Component Services snap-in, 329
Computer Management snap-in, 329
Device Manager snap-in, 81–93, 104–106, 329
Disk Management snap-in, 329, 372–377, 388
Event Viewer snap-in, 329, 513–517
Folder snap-in, 329
Group Policy Object Editor snap-in, 329
IP Security Monitor snap-in, 329
IP Security Policy Management snap-in, 329
Link to Web Address snap-in, 329
Local Computer Policy snap-in, 423
Local Users and Groups snap-in, 329
managing resources, 332–334
Network Access Protection Client Configuration snap-in, 329
Performance Monitor snap-in, 329, 517–521
Print Management snap-in, 329
Resultant Set of Policy snap-in, 329
Security Configuration and Analysis snap-in, 329
Security Templates snap-in, 329
Services snap-in, 329
Shared Folders snap-in, 330
snap-ins supported, 329–330
Task Scheduler snap-in, 330
Trusted Platform Module Management snap-in, 45, 330, 404
Windows Firewall with Advanced Security snap-in, 262, 264–274, 330
Windows Management Instrumentation Control snap-in, 330
Microsoft Office, 28
Microsoft Terminal Services Client (MSTSC), 301
Microsoft Update, 491
Microsoft Virtual PC, 182
Microsoft Virtual Server, 182
migrating from previous Windows version
about, 49–50
configuring accounts, 51–52
lesson summary, 64
migrating user data, 60–63
review questions and answers, 64–65, 76–77
running Setup Wizard, 50–51
transferring files with USMT, 56–60
transferring files with Windows Easy Transfer, 52–56
upgrading from Windows Vista, 52
upgrading from Windows XP, 52
migrating virtual machines, 204–206
Minimum Password Age setting, 424
Minimum Password Length setting, 424
mirrored volume type, 374–375, 377
MMC (Microsoft Management Console)
about, 328–329
ActiveX Control snap-in, 329
adding snap-ins, 330–332
Authorization Manager snap-in, 329
Certificates snap-in, 329, 402
Component Services snap-in, 329
Computer Management snap-in, 329
Device Manager snap-in, 81–93, 104–106, 329
Disk Management snap-in, 329, 372–377, 388
Event Viewer snap-in, 329, 513–517
Folder snap-in, 329
Group Policy Object Editor snap-in, 329
IP Security Monitor snap-in, 329
IP Security Policy Management snap-in, 329

Link to Web Address snap-in, 329
Local Computer Policy snap-in, 423
Local Users and Groups snap-in, 329
managing resources, 332–334
Network Access Protection Client Configuration snap-in, 329
Performance Monitor snap-in, 329, 517–521
Print Management snap-in, 329
Resultant Set of Policy snap-in, 329
Security Configuration and Analysis snap-in, 329
Security Templates snap-in, 329
Services snap-in, 329
Shared Folders snap-in, 330
snap-ins supported, 329–330
Task Scheduler snap-in, 330
Trusted Platform Module Management snap-in, 45, 330, 404
Windows Firewall with Advanced Security snap-in, 262, 264–274, 330
Windows Management Instrumentation Control snap-in, 330
Mobile Broadband Interface Model (MBIM) standard, 22
mobile devices
airplane mode, 481
configuring offline file synchronization, 473–476
configuring policy settings for offline files, 471–473
configuring settings for device power, 476–478
connecting with Wi-Fi Direct, 480
controlling metered connections, 226–227
lesson summary, 478
location-based services, 152, 481–482
managing BitLocker, 463–471
mobile broadband, 22
review questions and answers, 478–479, 485–486
sign-in considerations, 435
Modify permission
about, 353
managing file system objects, 394, 396
shared folders, 352
monitoring system health and performance
Performance Monitor, 517–521
Task Manager statistics, 502–510
Windows Action Center, 511–513
monitoring USB devices, 105–106
Move VM Wizard
about, 205
Choose Move Type page, 205
Choose Options For Moving Storage page, 206
MS-CHAP v2 (Microsoft CHAP Version 2), 319
MSConfig (Microsoft Configuration) utility
about, 508, 544
Boot tab, 545
General tab, 545
removing VHD installations, 71
Services tab, 545
Startup tab, 546
Tools tab, 546
MSIExec command
about, 120–121
additional information, 122
display options, 121
installation options, 121
logging options, 121
repair options, 121
restart options, 121
update options, 121
MSIFastInstall property (Windows Installer), 120
msinfo32 command, 93–95
MSTSC (Microsoft Terminal Services Client), 301
Mstsc.exe (Remote Desktop)
about, 298–299
Advanced tab, 307–308
configuring, 299–301
configuring multiple sessions, 305
Display tab, 302–303

Experience tab, 306–307
General tab, 302
lesson summary, 308
Local Resources tab, 303–305
opening, 301
Programs tab, 305
review questions and answers, 308–309, 338–339
Mulcare, Mike, 426
multicast addresses, 236
multiple partition systems, 39
My Printer Properties dialog box, 365

N

name resolution, configuring, 238–240
NAP (Network Access Protection) Client Configuration, 329
native applications and interface
about, 128
acquiring desktop apps in Windows Store, 131
controlling with AppLocker, 133–137
installing, 128–129
Internet Explorer 10 and, 148
inventorying, 139–140
lesson summary, 140
managing access to, 131–133
managing Windows Update, 494–496
practice exercises, 141–142
reinstalling, 129–130
removing, 139–140
review questions and answers, 140–141, 144
sideloading apps, 137–139
switching to, 507
Task Manager statistics, 506–507
uninstalling, 128–129
updating, 128–129
navigating user interface
about, 2–3
adding Windows administrative programs to Start screen, 7–8
closing applications, 11–12
managing Start screen, 3–7
switching between applications, 10–11
using charms, 8–10
Netsh command, 324–325
netstat command, 254–255
Network Access Protection (NAP) Client Configuration snap-in (MMC), 329
network adapters
adding second default gateway, 240–241
configuring IP settings, 233–237
configuring name resolution, 238–240
connecting to wireless networks, 241–246
dual TCP/IP stack and, 237–238
installing, 227–228
isatap.localdomain, 250
troubleshooting, 254, 313
virtual switches and, 213
network addresses, 237
Network and Sharing Center
about, 228–230
accessing from Control Panel, 228, 276, 310, 344–345
accessing from Start screen, 229
adding second default gateway, 240–241
configuring, 344–345
configuring IP settings, 232–237
configuring name resolution, 238–240
connecting to wireless networks, 241–246
dual TCP/IP stack, 237–238
managing network profiles, 230–232
sharing files and folders, 344–345
Troubleshooter option, 313–314
viewing network connections, 310–313
viewing network settings, 249–252
network discovery
about, 231–232, 276
creating profiles, 276–280

folder sharing settings, 347
Network metric, 503, 507
network troubleshooters, 252–254
networking and network connections
configuring, 223–247
connecting to VPNs, 315–321
lesson summaries, 246, 255
practice exercises, 256–257
Remote Assistance tool, 294–295
Remote Desktop tool, 298–299
review questions and answers, 246–247, 255–256, 258–259
Task Manager statistics, 503
testing, 236
transferring files via, 54–55
troubleshooting, 247–256, 310–314
viewing, 225–226, 310–313
for virtual machines, 208–210
Windows Firewall with Advanced Security and, 270–271, 273–274
wireless networks, 241–246
Networks taskbar, 242
New Inbound Rule Wizard, 270
New Virtual Machine Wizard
Assign Memory page, 198
Completing The New Virtual Machine Wizard page, 202
Configure Networking page, 198–199
Connect Virtual Hard Driver page, 199–200
Installation Options page, 200–201
opening, 195
Specify Name And Location page, 196–197
Before You Begin page, 195
NPIV (N_Port ID Virtualization), 210
N_Port ID Virtualization (NPIV), 210
NT LAN Manager (NTLM), 444, 449–450
NTFS permissions
about, 352–353
creating advanced security settings, 355–360
identifying, 360–361
modifying, 354–355
resolving conflicts, 362
resource ownership, 361–362
share-level permissions and, 400
NTLM (NT LAN Manager), 444, 449–450

O

offline caching, 533
Offline command (DiskPart), 388
offline files
configuring policy settings for, 471–473
configuring synchronization, 473–476
Offline Files dialog box
about, 474
Disk Usage tab, 475
Encryption tab, 475
General tab, 475
Network tab, 475
Offline Files Disk Usage dialog box, 475
Online command (DiskPart), 388
online services, accessing Photos application, 432
Open New Window option (apps), 5
Opera browser, 149
optimization, system, 507–508
Optimize Drives Optimization Schedule dialog box, 382
outbound rules, 271–272
Outlook.com application, 431
ownership of resources, 361–362, 399

P

package manifest, 139
packaged app rules, 134
Page File metric, 506
partitions
about, 373
actions supported, 375–376

creating on Windows To Go disks, 47
multiple partition systems, 39
types supported, 374
password considerations
administrator accounts, 283
displaying passwords, 163
HomeGroup feature, 280, 311
local accounts, 423
logging on with picture passwords, 432–435
Microsoft accounts, 431
name and password-based authentication, 422–424
Remote Assistance tool, 296
resource sharing and, 348
wireless networks, 282–283
Password Expiration setting, 424, 446
Password History Retention setting, 424
Pause task, 204
PEAP (Protected EAP), 319
percent processor time metric, 518
performance considerations
Driver Verifier utility and, 95
Performance Monitor, 329, 517–521
SMB 3, 224
Task Manager statistics, 504–506
troubleshooting, 18
performance counters, 518–519
Performance Monitor snap-in (MMC)
about, 329, 517
opening, 517–518
system diagnostics, 520–521
Permission Entry dialog box, 395–397
permissions
about, 438
for auditing, 400–402
documenting, 397
file system, 394–397
folder sharing, 350–352
groups and, 353, 356–358, 394, 397–400
inheritance and, 356, 358, 360, 397–399
MMC considerations, 333–334
NTFS, 352–362
printing, 366–367
Remote Assistance tool, 296
Remote Desktop tool, 307
share-level, 400
troubleshooting, 400
user rights versus, 438
viewing available, 395
Permissions dialog box, 354–355
Permissions Entry dialog box, 357
personal identification number (PIN)
about, 435
smart card authentication and, 425
phishing attacks, 285–286
Photos application, 431–432
picture passwords
about, 432, 434–435
changing, 434
creating, 432–433
logging on with, 432–435
removing, 434
PIN (personal identification number)
about, 435
smart card authentication and, 425
planning virtual machines
about, 192
establishing names and locations, 192–193
installation options, 194
memory availability considerations, 193–194
plug-ins (add-ons)
about, 13, 165
challenges using, 165
disabling, 171
enabling, 171
managing accelerators, 170
managing ActiveX controls, 166–169
managing search providers, 170
managing toolbars and extensions, 169–170
managing tracking protection, 170

managing with Group Policy, 172–175
preventing installation of, 173
specifying approved, 174–175
starting IE without, 171–172
Pnputil.exe tool, 102–103
Point-to-Point Protocol (PPP), 316
policies
BitLocker, 464–466
hardware, 107–114, 117
offline files, 471–473, 475
password, 283
power management for devices, 476–478
update, 499–500
ports, SMTP, 271–272
power management for devices
about, 88–89
configuring policy settings, 476–478
Power Off option, 204
Power Users menu
access Event Viewer, 513
accessing Task Manager, 502
accessing Windows Update, 488–489
PowerShell (Windows). *See also specific cmdlets*
about, 326–327
configuring multiple Remote Desktop sessions, 305
Hyper-V support, 188
managing BitLocker, 468
sideloading apps, 138–140
SMB 3 support, 224
usage examples, 327–328
PPP (Point-to-Point Protocol), 316
pre-staging drivers, 80
Preboot eXecution Environment (PXE), 190
press and hold action, 3
primary partition type, 374
principals
about, 356, 396
permissions and, 356–358, 399
User Rights elements, 442
principle of least privilege, 157
Print Management snap-in (MMC), 329
Print permission, 367
printers
configuring permissions, 366–367
managing default, 311
shared, 232, 276–277, 320, 364–367
troubleshooting, 313
private IP addresses, 236
private profiles
about, 265
creating, 276–277
folder sharing settings, 347–348
private virtual switches, 199, 210, 213
processes
canceling restoration, 539
ending, 503–504
Task Manager statistics, 503
profiles
about, 265
enabling folder sharing, 346–347
modifying, 265–267
network discovery, 276–280
selecting for firewall rules, 271
Program Compatibility troubleshooter, 123–124
Properties dialog box
AppLocker, 134–135, 137
Internet Protocol Version 6, 238
Local Security Settings tab, 438
shared files, 354–355
shared folders, 349–352
wireless networks, 244–246
Protected EAP (PEAP), 319
Protected Mode Compatibility Layer, 161
Protected Mode (IE)
about, 157–160
disabling, 161
Public Key policy, 426
public keys
authentication and, 444

- certificates and, 455

public profiles
- about, 266
- creating, 277
- folder sharing for, 348

PXE (Preboot eXecution Environment), 190

Q

quiescence, 187

Quota Entries for Volume dialog box, 406

Quota Settings dialog box, 405–406

quotas in file systems, 405–408

R

RAID-5 volume type, 373–375, 377

RD Gateway Server Settings dialog box, 307

RD Gateway servers, 307–308

RDP files, 302

Read & Execute permission
- about, 353
- managing file system objects, 394, 396

Read permission
- about, 353
- managing file system objects, 394, 396
- shared folders, 350, 352, 362

Read Speed metric, 505

Recover command (DiskPart), 388

recovery. *See* backup and restoration

Recovery Drive Wizard, 549

Refresh Your PC feature, 23, 539–540, 549

Reimer, Stand, 426

reinstalling native applications, 129–130

Rem command (DiskPart), 388

Remote Assistance dialog box, 295

Remote Assistance tool
- about, 294, 297
- initiating, 294–296
- lesson summary, 297
- review questions and answers, 298, 338
- usage overview, 296–297

Remote Assistance Wizard, 295

Remote Desktop Connection window
- Advanced tab, 307–308
- Display tab, 302–303
- Experience tab, 306–307
- General tab, 302
- Local Resources tab, 303–305
- Programs tab, 305
- Show Options arrow, 301

Remote Desktop (Mstsc.exe)
- about, 298–299
- Advanced tab, 307–308
- configuring, 299–301
- configuring multiple sessions, 305
- Display tab, 302–303
- Experience tab, 306–307
- General tab, 302
- lesson summary, 308
- Local Resources tab, 303–305
- opening, 301
- Programs tab, 305
- review questions and answers, 308–309, 338–339

Remote Desktop Services, 298–299, 441

remote management
- about, 293, 323
- configuring and managing connections, 309–310, 315–322
- lesson summaries, 297, 308, 322, 334
- Microsoft Management Console, 328–334
- Netsh tool, 324–325
- practice exercises, 335–337
- Remote Assistance tool, 294–298
- Remote Desktop tool, 298–309
- review questions and answers, 298, 308–309, 322–323, 334–335, 338–341
- troubleshooting problems, 310–314

Windows PowerShell, 326–328
Windows Remote Shell, 325–326
RemoteFX feature, 18
removable media
backing up data, 529
BitLocker To Go support, 404, 466, 470–471
creating storage space from, 410
disabling installation of, 110
transferring files via, 53–56
Remove-AppxPackage cmdlet, 139
Remove-AppxProvisionedPackage cmdlet, 139
Remove command (DiskPart), 388
removing native applications, 139–140
Repair command (DiskPart), 388
Rescan command (DiskPart), 388
reserved IP addresses, 236
Reset task (virtual machines), 204
Reset Your PC feature, 23, 539–543, 549
resizing tiles, 5–6
resource ownership, 361–362, 399
resource sharing
HomeGroup feature, 311
lesson summaries, 363, 367
Network and Sharing Center, 232
practice exercises, 368
review questions and answers, 363, 367–370
shared files, 232, 276–277, 320, 343–363
shared folders, 253, 277, 313, 343–363
shared printers, 232, 276–277, 320, 364–367
viewing, 93–94
resource utilization, 503
restart, disabling after failure, 552
restoration
for an entire computer, 535–536
from bad driver installation, 546–547
canceling process, 539
disabling restart after failure, 552
from File History backups, 533–535
Refresh method, 539–540
Reset method, 539, 541–543
of system images, 535–536
using System Restore, 536–539
restore points, 538
Resultant Set of Policy snap-in (MMC), 329
Resume-BitLocker cmdlet, 468
Retain command (DiskPart), 388
Reveal Password button, 163
rolling back
drivers, 91
updates, 497–499
rules
defining, 133–134
enforcing, 134–137
Windows Firewall, 274
Windows Firewall with Advanced Security, 269–274
"run as" task execution, 454–455
Run dialog box, 466, 471

S

SACLs (System Access Control Lists)
about, 392
auditing access to securable objects with, 400–402
SAN command (DiskPart), 388
sandbox attribute (HTML5), 157
SANs (storage area networks)
about, 208
assigning storage for virtual machines, 214–216
HBA technology, 210
ScanState.exe utility, 57–61
scheduling
backups, 529
drive optimization, 382–383
script rules, 133
SCSI controllers, 214–215

SDDL (security descriptor definition language), 445
Search charm, 9
search providers, 170
Second Level Address Translation (SLAT), 18, 185
Secure Boot feature, 22–23, 284–285
secure desktop environment, 444
Secure Socket Layer (SSL), 245, 455
security account manager database authentication, 422
security associations, 274
Security Configuration and Analysis snap-in (MMC), 329
security considerations
  administering authentication, 419–436
  administering authorization, 437–459
  configuring IE security settings, 156–164
  configuring network discovery, 275–280
  configuring wireless security, 280–283
  within file systems, 391–397
  Internet Protocol Security, 267–268
  lesson summaries, 274, 283, 286
  mobile devices and, 463–480
  network discovery, 276
  NTFS permissions, 352–362
  practice exercises, 287–289
  Remote Desktop tool, 299, 307
  review questions and answers, 275, 283–284, 287, 290–291
  Secure Boot, 284–285
  SmartScreen Filter, 285–286
  SMB 3, 224
  starting IE without add-ons, 171–172
  user rights assignments and, 439
  VPN connections, 315
  Wi-Fi Direct, 480
  Windows Firewall and exceptions, 261–274
  Windows Store and, 17
  Windows Update and, 488
  wireless networks, 245–246, 280–281
security descriptor definition language (SDDL), 445
security descriptors, 385
security identifier (SID), 447
security principals
  about, 356, 396
  permissions and, 356–358, 399
  User Rights elements, 442
Security Settings window
  Internet zone, 167
  Local Intranet zone, 168
Security Templates snap-in (MMC), 329
Select command (DiskPart), 388
Select Users Or Groups dialog box, 394
self-powered USB hubs, 105
Server Manager tool, 328
Server Message Block (SMB)
  enhancements in, 224–225
  local security settings, 447, 449
service accounts, 441, 457
service principal name (SPN), 444, 447
service set identification (SSID, 245
Services snap-in (MMC), 329
Set Default Programs page, 149–150
SetID command (DiskPart), 388
Settings charm
  about, 10
  accessing Control Panel, 132, 149, 276
  accessing user rights, 439
  accessing Windows RE, 550
  adding tiles to administrative tools, 7
  Change PC Settings option, 44, 132, 226, 312
  configuring IE, 151
  connecting to wireless networks, 241
  controlling metered connections, 226–227
  creating PINs, 435
  enabling folder sharing, 346
  manipulating locating settings, 482
  opening Device Manager, 82
  PC Info option, 30

restoring personal files, 533
system recovery, 540
viewing network connections, 224
Setup Backup dialog box, 529
setup classes for devices, 108–110
Setup Wizard
configuring accounts, 40–43, 51–52
starting installation, 38–39, 50–51
Share charm, 9
share-level permissions, 400
shared files
about, 343, 346–352
configuring Network and Sharing Center, 344–345
encryption and, 278, 348
File and Printer Sharing mechanism, 232, 276–277, 320, 347
NTFS permissions, 352–362
shared folders
about, 343, 346–352
configuring Network and Sharing Center, 344–345
network discovery profiles and, 277
NTFS permissions, 352–362
troubleshooting, 253, 313
Shared Folders snap-in (MMC), 330
shared printers
configuring, 364–367
File and Printer Sharing mechanism, 232, 276–277, 320, 347
shared resources
HomeGroup feature, 311
lesson summaries, 363, 367
Network and Sharing Center, 232
practice exercises, 368
review questions and answers, 363, 367–370
shared files, 232, 276–278, 320, 343–363
shared folders, 253, 277, 313, 343–363
shared printers, 232, 276–277, 320, 364–367
viewing, 93–94
Shrink command (DiskPart), 388–389
Shut Down option, 204
SID (security identifier), 447
sideloading apps, 137–139
sign-in process
about, 420–421
biometric authentication, 427–428
certificates and, 426
configuring Microsoft accounts, 430–431
lesson summary, 435
managing credentials, 428–430
mobile devices and, 435
practice exercises, 459–460
review questions and answers, 436–437, 461
single sign-on, 422, 430
smart card authentication, 425–427
user name and password-based authentication, 422–424
using picture passwords, 432–435
using PINs, 435
signed drivers, 81
Sigverif.exe utility, 81
simple volume type, 374
single sign-on (SSO), 422, 430
SkyDrive feature, 19–20, 430–432
SLAT (Second Level Address Translation), 18, 185
Sleep action, 45
slide action, 3
slmgr command, 138
Smaller (or Larger) option (apps), 5
smart cards
about, 425
authentication for, 425–427
SmartScreen Filter feature, 285–286
SMB (Server Message Block)
enhancements in, 224–225
local security settings, 447, 449
SMB Transparent Failover, 224
SMTP ports, 271–272
snap-ins (MMC)
ActiveX Control snap-in, 329

adding, 330–332
adding multiple instances of, 332
adding snap-ins, 330–332
Authorization Manager snap-in, 329
Certificates snap-in, 329, 402
Component Services snap-in, 329
Computer Management snap-in, 329
Device Manager snap-in, 81–93, 104–106, 329
Disk Management snap-in, 329, 372–377, 388
Event Viewer snap-in, 329, 513–517
Folder snap-in, 329
Group Policy Object Editor snap-in, 329
IP Security Monitor snap-in, 329
IP Security Policy Management snap-in, 329
Link to Web Address snap-in, 329
listing of, 329–330
Local Computer Policy snap-in, 423
Local Users and Groups snap-in, 329
managing resources with, 332–334
Network Access Protection Client Configuration snap-in, 329
Performance Monitor snap-in, 329, 517–521
Print Management snap-in, 329
Resultant Set of Policy snap-in, 329
Security Configuration and Analysis snap-in, 329
Security Templates snap-in, 329
Services snap-in, 329
Shared Folders snap-in, 330
Task Scheduler snap-in, 330
Trusted Platform Module Management snap-in, 45, 330, 404
Windows Firewall with Advanced Security snap-in, 262, 264–274, 330
Windows Management Instrumentation Control snap-in, 330

snapshots
System Restore and, 537
virtual machine, 204

solid state drives (SSDs), 193–194, 205

spanned volume type, 374, 376

Special Permissions permission
managing file system objects, 394
printers and, 367

SPN (service principal name), 444, 447

Spotfix feature, 384

SSDs (solid state drives), 193–194, 205

SSL (Secure Socket Layer), 245, 455

SSO (single sign-on), 422, 430

Stanek, William, 426

Start charm, 10

Start screen
about, 2
accessing Control Panel, 489
accessing Disk Cleanup, 378
accessing Event Viewer, 513
accessing Network and Sharing Center, 229, 345
accessing Refresh method, 540
accessing Remote Assistance, 294–295
accessing Remote Desktop, 300–301
adding tiles for administrative tools, 7–8
connecting to VPNs, 315
controlling IE behavior, 150–151, 155
managing, 3–7
manipulating apps on, 5–6
opening, 11
opening Device Manager from, 82
opening IE, 147–148

startup key storage, 469, 471

startup memory, 198

startup system disks, 50

state-changing tasks (VMs), 204

storage area networks (SANs)
about, 208
assigning storage for virtual machines, 214–216
HBA technology, 210

storage management
Chkdsk utility, 383–386

disk management and, 371–380
DiskPart utility, 66–69, 386–390
lesson summary, 390, 413
Microsoft Drive Optimizer tool, 380–383
review questions and answers, 390–391, 413–414, 416, 418
startup key storage, 469, 471
Storage Spaces feature, 409–414
for virtual machines, 193–194, 204–206, 208–210, 214–216
Storage Spaces feature
about, 409–410
benefits of, 413
creating storage spaces, 410–413
lesson summary, 413
practice exercises, 415
review questions and answers, 413–414, 418
storage space size constraints, 412
storage virtualization, 412–413
striped volume type, 374–376
subnet masks, 234
Suspend-BitLocker cmdlet, 468
swipe action, 3
switches, virtual
about, 199, 203, 210–213
assigning to virtual machines, 213–214
MAC addresses and, 209
switching between applications, 10–11
symbolic links, 441, 444
Sync Center, 473–474
synchronization
configuring for offline files, 473–476
guest enlightenment and, 187
of settings between devices, 20
System Access Control Lists (SACLs)
about, 392
auditing access to securable objects with, 400–402
system diagnostics, 520–521
System Disk metric, 506
system disks, 50
system files, 379
System group, 392
system images
backing up, 530
restoring, 535–536
System Information utility, 93–95
system optimization, 507–508
System Properties dialog box, 44, 300, 537–538
system protection and recovery
advanced recovery and restoration options, 548–553
advanced settings and features, 544–548
backup and restoration, 528–544
lesson summaries, 543, 547, 552
practice exercises, 553–554
review questions and answers, 543–544, 547–548, 552–553, 555–557
system repair or recovery disc, 549–550
System Restore
about, 536–539
configuring, 537–538
creating restore points, 538
enabling, 539

T

tap action, 3
Task Manager
about, 247–248, 502
Active Time metric, 505
App history tab, 506–507
Average Response Time metric, 505
Capacity metric, 505
CPU metric, 503
CPU Time metric, 506
Details tab, 509–510
Disk metric, 503
Formatted metric, 505
Memory metric, 503

Metered Network metric, 507
Network metric, 503, 507
Page File metric, 506
Performance tab, 248, 504–506
Processes tab, 248, 503–504
Read Speed metric, 505
Services tab, 510
Startup tab, 507–508, 546
System Disk metric, 506
Tile Updates metric, 507
Transfer Rate metric, 506
Users tab, 508
Write Speed metric, 505
Task Scheduler snap-in (MMC), 330
taskbar (desktop), 344
TCP/IP (Transmission Control Protocol/Internet Protocol)
adding second default gateway, 240
configuring name resolution, 239
dual stack, 237–238
VPNs and, 320
TechNet forums, 185, 187
Temporal Key Integrity Protocol (TKIP), 281
Temporary Internet Files (TIFs), 377–378
Teredo Tunneling Pseudo-Interface, 250
Terminal Services, 298
testing
for application compatibility, 122–123, 184
applications using Windows To Go, 48
Driver Verify utility support, 95–96
enabling Hyper-V for, 184
network connectivity, 236
starting IE without add-ons, 171–172
thin-provisioned VHD files, 67
thumbnail files, 378
TIFs (Temporary Internet Files), 377–378
Tile Updates metric, 507
tiles
adding for administrative tools, 7–8
controlling IE Start screen behavior, 150–151, 155
live, 2
manipulating, 4–5
resizing, 5–6
TKIP (Temporal Key Integrity Protocol), 281
toolbars, 169–170
touchscreens
accessing Edge UI, 8
add-ons and, 165
Internet Explorer 10 and, 12, 145–153
picture passwords and, 435
switching between applications, 10
terminology used, 3
TPM (Trusted Platform Module) Management snap-in (MMC)
BitLocker and, 404, 464, 468–470
Windows To Go and, 45, 330
tracking protection, 170
Transfer Rate metric, 506
transferring files
migrating user data, 60–63
via User State Migration Tool, 56–60
via Windows Easy Transfer, 53–56
Transmission Control Protocol/Internet Protocol (TCP/IP)
adding second default gateway, 240
configuring name resolution, 239
dual stack, 237–238
VPNs and, 320
troubleshooting
bandwidth considerations in, 106
documentation and, 322
hardware problems, 89–92, 95, 104, 367
HomeGroup feature, 253, 313
IP addresses, 233, 313
network adapters, 254, 313
network problems, 247–256, 310–314
performance issues, 18
permissions, 400

printers, 313, 367
program compatibility, 123–125, 184
Remote Assistance tool and, 297
Remote Desktop tool and, 299
shared folders, 253, 313
starting IE without add-ons, 171–172
System Restore and, 536–539
Task Manager and, 502–510
View Update History window and, 497
Trusted Boot, 22–23
Trusted Platform Module (TPM) Management snap-in (MMC)
about, 330
BitLocker and, 404, 464, 468–470
Windows To Go and, 45
trusted sites, adding to IE, 162
Trusted Sites dialog box, 162
trusted user accounts, 439
Turn Live Tile Off option (apps), 5
Turn Off task, 204
Type 1 hypervisors, 182
Type 2 hypervisors, 182

U

UAC Settings dialog box, 453
UAC (user account control)
Protected Mode and, 160
running tasks and, 452–455
as Windows Action Center source, 511
UEFI (Unified Extensible Firmware Interface), 22–23, 284–285
UI (user interface). *See also* touchscreens
improvements in, 1
Internet Explorer 10 and, 146–153
navigating, 2–25
setting up Windows To Go from, 45–46
UNC (Universal Naming Convention), 189, 350, 528
Understanding IPv6 (Davies), 236
unicast response, 267
Unified Communications certificates, 455
Unified Extensible Firmware Interface (UEFI), 22–23, 284–285
Uninstall option (apps), 5
uninstalling
drivers, 91
native applications, 128–129
updates, 497–499
UniqueID command (DiskPart), 388
Universal Naming Convention (UNC), 189, 350, 528
Unlock-BitLocker cmdlet, 468
unmetered connections, 492
Unpin From Start option (apps), 5
unsigned drivers, 81
updates
accessing settings, 488–490
classes of, 491
configuring policies, 499–500
configuring settings, 490–493
for drivers, 91
identifying new, 493–494
lesson summary, 500
managing in native interface, 494–496
for native applications, 128–129
practice exercises, 522
review questions and answers, 500–501, 524
rolling back, 497–499
viewing update history, 496–497
upgrading to Windows 8
about, 49–50
configuring accounts, 51–52
lesson summary, 64
migrating user data, 60–63
review questions and answers, 64–65, 76–77
running Setup Wizard, 50–51
transferring files with USMT, 56–60
transferring files with Windows Easy Transfer, 52–56
upgrading from Windows Vista, 52

upgrading from Windows XP, 52
USB devices
monitoring, 105–106
startup key storage, 469, 471
transferring files via, 55–56
Windows To Go and, 21, 44–46
USB DVD Download tool, 50
user account control (UAC)
Protected Mode and, 160
running tasks and, 452–455
as Windows Action Center source, 511
user accounts
adding sideloaded apps to, 138
assigning certificates, 457
authenticating, 420–428
DACLs and, 394
default ownership of shared resources, 361
disk quotas for, 407–408
Remote Desktop connections and, 299, 301
trusted, 439
user rights and, 437–443
user interface (UI). *See also* touchscreens
improvements in, 1
Internet Explorer 10 and, 146–153
navigating, 2–25
setting up Windows To Go from, 45–46
user name and password-based authentication, 422–424
user rights
about, 437–438
assigning, 437–443
permissions versus, 438
working in groups, 438
User State Migration Tool (USMT)
about, 56–60
migrating user data, 60–63
Users group, 392
USMT (User State Migration Tool)
about, 56–60
migrating user data, 60–63
USN journals, 385

V

verifier command, 95–101
verifying
availability of device driver software, 426
existing groups, 394
IP addresses, 234
VHDs (virtual hard disks)
about, 65–66
assigning storage for virtual machines, 214–216
creating from existing installations, 66–68
creating using DiskPart, 68–69
creating virtual machines and, 199–200
lesson summary, 72
memory considerations, 194
migrating virtual machines and, 204, 206
practice exercises, 74–75
removing installations, 71–72
review questions and answers, 72–73, 78
starting system from, 69–71
VHDX format
assigning storage for virtual machines, 214–216
creating virtual machines and, 199–200
memory considerations, 193–194
migrating virtual machines and, 204, 206
View Update History window, 496–497
viewing
available permissions, 395
device and driver information, 83–88
network connections, 225–226, 310–313
network settings, 249–252
resource conflicts, 93–94
shared resources, 93–94
update history, 496–497
Windows Action Center, 511–512
Windows Firewall with Advanced Security configuration, 265
virtual consoles, 203–204

Virtual Fibre Channel
- about, 208
- assigning storage for virtual machines, 214–216
- HBA technology, 210
- WWNs, 210

virtual hard disks (VHDs)
- about, 65–66
- assigning storage for virtual machines, 214–216
- creating from existing installations, 66–68
- creating using DiskPart, 68–69
- creating virtual machines and, 199–200
- lesson summary, 72
- memory considerations, 194
- migrating virtual machines and, 204, 206
- practice exercises, 74–75
- removing installations, 71–72
- review questions and answers, 72–73, 78
- starting system from, 69–71

virtual local area networks (VLANs), 211

Virtual Machine Connection view, 203–204, 213

virtual machine snapshots, 204

virtual machines (VMs)
- about, 17, 182
- configuring, 206, 208–217
- core resources, 183
- creating, 191–192, 195–202
- guest enlightenment and, 187
- hardware requirements, 17, 193, 200, 208–210
- Hyper-V overview, 182–191
- Hyper-V virtual switch, 210–216
- installing operating systems in, 203–204
- lesson summary, 206–207, 216
- licensing considerations, 185
- memory requirements, 18, 185, 193–194, 198
- migrating to other storage resources, 204–206
- planning, 192–194
- practice exercises, 217–218
- review questions and answers, 207, 217, 219–221
- state-changing tasks, 204
- storage and networking for, 193–194, 204–206, 208–210, 214–216
- using, 202–206

Virtual PC Guy Blog, 188

Virtual PC (Microsoft), 182

virtual ports, 203

virtual private networks (VPNs), 315–322

Virtual Server (Microsoft), 182

Virtual Switch Manager (Hyper-V), 209

virtual switches
- about, 199, 203, 210–213
- assigning to virtual machines, 213–214
- MAC addresses and, 209

virtualization. *See* Hyper-V; virtual machines

virtualized media, 189–190

VLANs (virtual local area networks), 211

VMs (virtual machines)

about, 17, 182
- configuring, 206, 208–217
- core resources, 183
- creating, 191–192, 195–202
- guest enlightenment and, 187
- hardware requirements, 17, 193, 200, 208–210
- Hyper-V overview, 182–191
- Hyper-V virtual switch, 210–216
- installing operating systems in, 203–204
- lesson summary, 206–207, 216
- licensing considerations, 185
- memory requirements, 18, 185, 193–194, 198
- migrating to other storage resources, 204–206
- planning, 192–194
- practice exercises, 217–218
- review questions and answers, 207, 217, 219–221
- state-changing tasks, 204
- storage and networking for, 193–194, 204–206, 208–210, 214–216

using, 202–206
volumes
actions supported, 375–376
changing size of, 376
types supported, 374–375
VPN Connection Properties dialog box
about, 315
General tab, 316
Networking tab, 319–320
Options tab, 316–317
Security tab, 317–319
Sharing tab, 320–321
VPNs (virtual private networks), 315–322

W

WDDM (Windows Display Driver Model), 29–30
Weather app, 481
web credentials, 430
WEP (Wired Equivalent Privacy), 281
White, Byron, 426
Wi-Fi Direct, 480
Wi-Fi Protected Access v2 (WPA2), 281, 283
Wi-Fi Protected Access (WPA), 281
Windows 7
File Recovery Wizard, 529
Hyper-V support, 187
Windows 8 editions
about, 25
architecture differences in, 28–29
hardware requirements for, 29–31
Hyper-V support, 187, 190
lesson summary, 31
practice exercises, 32–33
product differences in, 26–28
review questions and answers, 31–32, 34–35
Windows Action Center
modifying settings for, 512–513
sources for, 511
viewing, 511–512
Windows Defender system protection tool, 495
Windows Deployment Services, 190
Windows Display Driver Model (WDDM), 29–30
Windows Easy Transfer tool, 52–56
Windows Firewall
about, 262
configuration options, 262–263
configuring to allow specific apps, 263–264
monitoring rules configured by, 274
removing apps from configuration, 264
as Windows Action Center source, 511
Windows Firewall with Advanced Security snap-in (MMC)
about, 262, 264–265, 330
allowing secure connections, 270–271
configuring connection security rules, 273–274
configuring inbound rules, 269
configuring IPsec settings, 267–268
configuring outbound rules, 271–272
modifying firewall profile, 265–267
viewing initial configuration, 265
Windows Installer
about, 120
MSIFastInstall property, 120
running, 120–122
Windows Installer rules, 133
Windows Live ID, 16
Windows Live Messenger, 430
Windows Management Instrumentation (WMI) Control snap-in (MMC), 330
Windows PowerShell. *See also specific cmdlets*
about, 326–327
configuring multiple Remote Desktop sessions, 305
Hyper-V support, 188
managing BitLocker, 468
sideloading apps, 138–140
SMB 3 support, 224
usage examples, 327–328

Windows Recovery Environment (Windows RE), 45, 550–552
Windows Remote Shell (WinRS), 325–326
Windows RT operating system
  Microsoft Office and, 28
  Windows Store and, 14
  WinRT and, 4
Windows Runtime (WinRT) environment, 3–4
Windows Server 2003, 187
Windows Server 2008, 182, 187
Windows Server 2008 Active Directory Resource Kit (Reimer et al.), 426
Windows Server 2012
  Group Policy Management Console, 153–154
  Hyper-V in, 18–19, 182, 187, 190
Windows Server Update Services (WSUS), 499–500
Windows Setup dialog box, 38–39
Windows Store
  acquiring desktop apps, 131
  adding applications from, 14–17
  cloud connectivity and, 19
  disabling and controlling access to apps, 131
  reinstalling apps, 129–130
Windows To Go
  about, 21
  creating partitions on disks, 47
  installing Windows 8 with, 44–48
  testing applications using, 48
Windows Update
  accessing settings, 488–490
  classes of updates, 491
  configuring policies, 499–500
  configuring settings, 490–493
  identifying new updates, 493–494
  importance of, 488
  lesson summary, 500
  managing in native interface, 494–496
  practice exercises, 522
  review questions and answers, 500–501, 524
  rolling back updates, 497–499
  viewing update history, 496–497
  as Windows Action Center source, 511
Windows Vista
  accessing Remote Desktop tool, 300
  Hyper-V support, 187
  upgrading from, 52–53, 57
Windows XP
  Hyper-V support, 187
  upgrading from, 52–53, 57
WinRS (Windows Remote Shell), 325–326
WinRT (Windows Runtime) environment, 3–4
Wired Equivalent Privacy (WEP), 281
wireless networks
  connecting to, 241–244
  managing, 244–246
  security considerations, 280–281
  viewing details, 251–252
WMI (Windows Management Instrumentation) Control, 330
WORKGROUP work group, 44
working sets, 441
World Wide Names (WWNs), 210
WPA (Wi-Fi Protected Access), 281
WPA2 (Wi-Fi Protected Access v2), 281, 283
Write permission
  about, 353
  managing file system objects, 394, 396
  shared folders, 350, 362
Write Speed metric, 505
WS-Management standard, 325
WSUS (Windows Server Update Services), 499–500
WWNs (World Wide Names), 210

X

XP Mode feature, 18