

EXAM ✓ **CRAM**

# MCTS

## 70-680

Microsoft Windows 7,  
Configuring

CD FEATURES 2 COMPLETE SAMPLE EXAMS



PEARSON

PATRICK REGAN

**EXAM** ✓ **CRAM**

# **MCTS 70-680**

**Microsoft Windows 7,  
Configuring**

**Patrick Regan**

## **MCTS 70-680 Exam Cram: Microsoft Windows 7, Configuring**

Copyright © 2011 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-4734-1

ISBN-10: 0-7897-4734-0

Library of Congress Cataloging-in-Publication data is on file.

Printed in the United States of America

First Printing: March 2011

### **Trademarks**

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

### **Warning and Disclaimer**

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

### **Bulk Sales**

Pearson offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

#### **U.S. Corporate and Government Sales**

**1-800-382-3419**

**corpsales@pearsontechgroup.com**

For sales outside of the U.S., please contact

#### **International Sales**

**international@pearsoned.com**

### **Associate**

#### **Publisher**

David Dusthimer

### **Acquisitions Editor**

Betsy Brown

### **Senior Development Editor**

Christopher

Cleveland

### **Managing Editor**

Sandra Schroeder

### **Project Editor**

Seth Kerney

### **Copy Editor**

The Wordsmithery  
LLC

### **Indexer**

Tim Wright

### **Proofreader**

Water Crest  
Publishing

### **Technical Editor**

Chris Crayton

### **Publishing Coordinator**

Vanessa Evans

### **Multimedia Developer**

Dan Scherf

### **Designer**

Gary Adair

### **Page Layout**

Studio Galou, LLC

# Contents at a Glance

	Introduction	1
<b>CHAPTER 1</b>	Introduction to Windows 7	23
<b>CHAPTER 2</b>	Installing, Upgrading, and Migrating to Windows 7	59
<b>CHAPTER 3</b>	System Management	107
<b>CHAPTER 4</b>	Disk Management	157
<b>CHAPTER 5</b>	Configuring Windows Networking	193
<b>CHAPTER 6</b>	Configuring Advanced Windows Networking	223
<b>CHAPTER 7</b>	Configuring Windows Firewall and Windows Defender	255
<b>CHAPTER 8</b>	User Management	281
<b>CHAPTER 9</b>	Managing Files and Folders	319
<b>CHAPTER 10</b>	Sharing Files and Folders	363
<b>CHAPTER 11</b>	Managing and Sharing Printers	391
<b>CHAPTER 12</b>	Working with Applications	419
<b>CHAPTER 13</b>	Working with Internet Explorer 8.0	445
<b>CHAPTER 14</b>	Mobile Computers and Remote Management	475
<b>CHAPTER 15</b>	Optimizing Windows 7 Systems	515
<b>CHAPTER 16</b>	Backups and System Recovery	535
	Practice Exam	573
	Index	591

# Table of Contents

<b>Introduction</b> . . . . .	<b>1</b>
The Value of Certification . . . . .	1
The Microsoft Certification Program . . . . .	3
Microsoft Certified Technology Specialist . . . . .	5
Microsoft Certified IT Professional . . . . .	6
Microsoft Certified Technology Specialist: Windows 7 Configuration . . . . .	6
Taking a Certification Exam . . . . .	14
How to Prepare for an Exam . . . . .	15
Day of the Exam . . . . .	17
Dealing with Test Anxiety . . . . .	20
Additional Resources . . . . .	21

## **CHAPTER 1:**

<b>Introduction to Windows 7</b> . . . . .	<b>23</b>
The Road to Windows 7 . . . . .	24
Defining Windows 7 . . . . .	27
Windows 7 Flavors . . . . .	28
Cram Quiz . . . . .	31
Cram Quiz Answers . . . . .	32
Windows 7 Graphical User Interface . . . . .	33
Working with the Desktop . . . . .	35
Windows 7 Taskbar . . . . .	37
Windows 7 Start Menu . . . . .	38
The Notification Area . . . . .	42
Customizing the Taskbar and Start Menu . . . . .	44
Working with Open Windows . . . . .	47
Gadgets . . . . .	49
Aero Desktop Experience . . . . .	50
Cram Quiz . . . . .	52
Cram Quiz Answers . . . . .	53
Review Questions . . . . .	54
Review Question Answers . . . . .	56

## **CHAPTER 2:**

<b>Installing, Upgrading, and Migrating to Windows 7</b> . . . . .	<b>59</b>
Installing Windows 7 . . . . .	60

Windows 7 Installation Methods . . . . .	62
Windows Clean Installation . . . . .	63
Upgrading Windows. . . . .	63
Windows Updates . . . . .	68
Activating Windows 7 . . . . .	70
Restore a Computer to a Previous Windows Installation . . . . .	70
Using BCDEdit . . . . .	71
Enabling a Dual-Boot System . . . . .	75
Cram Quiz . . . . .	76
Cram Quiz Answers . . . . .	77
Windows Easy Transfer and Windows User State Migration Tool . . . . .	78
Cram Quiz . . . . .	81
Cram Quiz Answers . . . . .	82
Deploying Windows 7 . . . . .	83
Windows Automated Installation Kit . . . . .	84
Windows PE. . . . .	84
Disk Cloning and the System Preparation Tool . . . . .	85
The Unattended Installation. . . . .	87
Installing Windows Using Windows System Image Manager . . . . .	87
Deploying Windows with WIM Images . . . . .	88
Deployment Image Servicing and Management . . . . .	91
Windows Deployment Services . . . . .	94
Cram Quiz . . . . .	95
Cram Quiz Answers . . . . .	95
Booting with a VHD Image . . . . .	96
Cram Quiz . . . . .	101
Cram Quiz Answers . . . . .	101
Review Questions . . . . .	102
Review Question Answers . . . . .	105

### **CHAPTER 3:**

#### **System Management . . . . . 107**

Configuring and Managing Windows . . . . .	108
Viewing Basic Information . . . . .	111
Changing Computer Name and Domain/Workgroup . . . . .	112
Windows Features and Programs . . . . .	113
Configuring Accessibility . . . . .	116
Parental Controls . . . . .	118
Cram Quiz . . . . .	120

Cram Quiz Answers . . . . .	121
Device Drivers . . . . .	122
Plug and Play Devices . . . . .	124
Signed Drivers . . . . .	124
Devices and Printers Folder . . . . .	125
Device Manager . . . . .	127
Adding a Device . . . . .	129
Configuring Keyboard and Mouse . . . . .	129
Managing Sound . . . . .	130
Cram Quiz . . . . .	132
Cram Quiz Answers . . . . .	133
Display Settings . . . . .	134
Desktop Themes . . . . .	136
Adjusting the Screen Settings . . . . .	137
Multiple Monitors . . . . .	140
Windows Aero . . . . .	141
Cram Quiz . . . . .	143
Cram Quiz Answers . . . . .	143
Advanced Windows Configuration . . . . .	144
Microsoft Management Console . . . . .	145
Administrative Tools . . . . .	145
Services . . . . .	146
Local and Group Policies . . . . .	148
The Registry . . . . .	149
Cram Quiz . . . . .	151
Cram Quiz Answers . . . . .	151
Review Questions . . . . .	152
Review Question Answers . . . . .	154

**CHAPTER 4:**

<b>Disk Management . . . . .</b>	<b>157</b>
Disk Management Tools . . . . .	158
Disk Partitioning . . . . .	161
Disk Storage Management . . . . .	162
File Systems . . . . .	167
Cram Quiz . . . . .	168
Cram Quiz Answers . . . . .	168
Working with Volumes . . . . .	169

Simple Volumes . . . . .	171
Spanned Volumes . . . . .	172
Extending Simple or Spanned Volumes . . . . .	173
Shrinking Volumes . . . . .	174
Striped Volumes . . . . .	174
Mirrored Volumes . . . . .	176
Mount Points. . . . .	179
Formatting Disks . . . . .	180
Cram Quiz . . . . .	180
Cram Quiz Answers . . . . .	181
Optimizing the Disk . . . . .	182
Monitoring Disk Space . . . . .	183
Running Check Disk . . . . .	183
Defragging the Hard Drive. . . . .	184
NTFS Disk Quotas. . . . .	185
Cram Quiz . . . . .	187
Cram Quiz Answers . . . . .	187
Review Questions . . . . .	188
Review Questions Answers . . . . .	190

**CHAPTER 5:**

**Configuring Windows Networking . . . . . 193**

Introduction to TCP/IP . . . . .	194
IPv4 TCP/IP Addressing . . . . .	195
IPv6 TCP/IP Addressing . . . . .	198
Default Gateway. . . . .	202
Name Resolution . . . . .	202
DHCP Services . . . . .	204
IP Configuration on Windows 7 Machines . . . . .	205
Network and Sharing Center . . . . .	208
Using the netsh Command . . . . .	208
Cram Quiz . . . . .	210
Cram Quiz Answers . . . . .	211
Tools to Help Diagnose Network Problems . . . . .	212
Cram Quiz . . . . .	217
Cram Quiz Answers . . . . .	217
Review Questions . . . . .	218
Review Question Answers . . . . .	220



**CHAPTER 6:**

<b>Configuring Advanced Windows Networking</b> . . . . .	<b>223</b>
Wireless Connection . . . . .	224
Configuring Wireless Networks . . . . .	227
Network Locations . . . . .	233
Cram Quiz . . . . .	234
Cram Quiz Answers . . . . .	235
Remote Access . . . . .	236
Dial-Up Connection . . . . .	237
Broadband Connection . . . . .	241
Virtual Private Networking . . . . .	242
DirectAccess . . . . .	246
Review Questions . . . . .	249
Review Question Answers . . . . .	252

**CHAPTER 7:**

<b>Configuring Windows Firewall and Windows Defender</b> . . . . .	<b>255</b>
Spyware and Windows Defender . . . . .	256
Cram Quiz . . . . .	263
Cram Quiz Answers . . . . .	263
Windows Firewall . . . . .	264
Basic Configuration . . . . .	266
Windows Firewall with Advanced Security . . . . .	269
Computer Connection Security Rules . . . . .	272
Cram Quiz . . . . .	275
Cram Quiz Answers . . . . .	275
Review Questions . . . . .	276
Review Question Answers . . . . .	279

**CHAPTER 8:**

<b>User Management</b> . . . . .	<b>281</b>
Authentication and Authorization . . . . .	282
User Accounts and Groups . . . . .	284
Managing Local Logon Accounts . . . . .	289
Credential Manager . . . . .	295
Cram Quiz . . . . .	296
Cram Quiz Answers . . . . .	297

User Account Control . . . . .	298
Cram Quiz . . . . .	307
Cram Exam Answers . . . . .	308
Security Auditing . . . . .	309
Cram Quiz . . . . .	313
Cram Exam Answers . . . . .	313
Review Questions . . . . .	314
Review Question Answers . . . . .	316

**CHAPTER 9:**

<b>Managing Files and Folders . . . . .</b>	<b>319</b>
NTFS . . . . .	320
NTFS Permissions . . . . .	321
Copying and Moving Files . . . . .	326
Folder and File Owners . . . . .	326
Controlling Who Can Access a USB Flash Device . . . . .	327
Cram Exam . . . . .	327
Cram Exam Answers . . . . .	328
Windows 7 File Structure . . . . .	329
Libraries . . . . .	331
Folder Options . . . . .	334
Searching in Windows . . . . .	336
Cram Exam . . . . .	340
Cram Exam Answers . . . . .	341
Encryption . . . . .	342
Encryption File System . . . . .	343
BitLocker Drive Encryption . . . . .	348
BitLocker To Go . . . . .	352
Cram Quiz . . . . .	353
Cram Quiz Answers . . . . .	354
Compression . . . . .	355
Compressed (Zipped) Folders . . . . .	355
NTFS Compression . . . . .	356
Cram Quiz . . . . .	357
Cram Quiz Answer . . . . .	357
Review Questions . . . . .	358
Review Question Answers . . . . .	360

**CHAPTER 10:**

<b>Sharing Files and Folders</b> . . . . .	<b>363</b>
Sharing Files and Folders . . . . .	364
Network Discovery and Browsing . . . . .	366
Sharing Folders . . . . .	369
Special and Administrative Shares . . . . .	374
Homegroup . . . . .	375
Managing Shares . . . . .	379
Connecting to a Shared Folder . . . . .	379
Cram Quiz . . . . .	381
Cram Quiz Answers . . . . .	382
BranchCache . . . . .	383
Cram Quiz . . . . .	385
Cram Quiz Answers . . . . .	385
Review Questions . . . . .	386
Review Question Answers . . . . .	388

**CHAPTER 11:**

<b>Managing and Sharing Printers</b> . . . . .	<b>391</b>
Printer in Windows . . . . .	392
Local Versus Network Printing . . . . .	394
Printing Process . . . . .	395
Installing a Printer on Windows 7 . . . . .	396
Printer Properties . . . . .	401
Location-Aware Printing . . . . .	403
Printer Permissions . . . . .	404
Managing the Print Spooler . . . . .	405
Managing Print Jobs . . . . .	407
Looking at the Logs . . . . .	408
Auditing Printer Access . . . . .	409
Troubleshooting Printing Problems . . . . .	410
Cram Quiz . . . . .	412
Cram Quiz Answers . . . . .	413
Review Questions . . . . .	414
Review Question Answers . . . . .	416

**CHAPTER 12:**

<b>Working with Applications</b> . . . . .	<b>419</b>
Windows Live Essentials . . . . .	420

Cram Quiz . . . . .	421
Cram Quiz Answer . . . . .	421
Application Compatibility . . . . .	422
Microsoft Application Compatibility Toolkit (ACT) and Shims . . . . .	425
XP Mode . . . . .	427
Cram Quiz . . . . .	430
Cram Quiz Answers . . . . .	430
Software Restrictions. . . . .	431
Cram Quiz . . . . .	438
Cram Quiz Answers . . . . .	439
Review Questions . . . . .	440
Review Question Answers . . . . .	442
<b>CHAPTER 13:</b>	
<b>Working with Internet Explorer 8.0 . . . . .</b>	<b>445</b>
Features of Internet Explorer 8.0 . . . . .	446
Internet Explorer Zoom . . . . .	448
Common Internet Explorer Settings. . . . .	449
Plug-Ins/Add-Ons and Scripting Languages. . . . .	452
Internet Explorer Security Features . . . . .	454
Using Offline Mode and Saving Webpages . . . . .	464
RSS Feeds . . . . .	465
Reset Internet Explorer to Default Settings . . . . .	466
Compatibility View Mode . . . . .	467
Using Accelerators . . . . .	467
Search Providers. . . . .	469
Cram Exam . . . . .	469
Cram Exam Answers . . . . .	470
Review Questions . . . . .	471
Review Question Answers . . . . .	473
<b>CHAPTER 14:</b>	
<b>Mobile Computers and Remote Management . . . . .</b>	<b>475</b>
Control Panel and Windows Mobility Center . . . . .	476
Configuring Presentation Settings for Mobile PCs . . . . .	478
Power Management . . . . .	481
File and Data Synchronization . . . . .	486
Windows SideShow . . . . .	492
Remote Projector . . . . .	493

Cram Quiz . . . . .	494
Cram Quiz Answers . . . . .	495
Remote Desktop and Remote Assistance . . . . .	496
Remote Desktop and Remote Desktop Connections . . . . .	497
Using Remote Assistance . . . . .	501
Using Administrative Tools for Remote Hosts . . . . .	502
Cram Quiz . . . . .	503
Cram Exam Answers . . . . .	504
PowerShell . . . . .	505
Cram Quiz . . . . .	509
Cram Quiz Answers . . . . .	509
Review Questions . . . . .	510
Review Question Answers . . . . .	513

**CHAPTER 15:**

<b>Optimizing Windows 7 Systems . . . . .</b>	<b>515</b>
Windows Performance Monitoring Tools . . . . .	516
Task Manager . . . . .	517
Resource Monitor . . . . .	519
Performance Monitor . . . . .	520
Windows Experience Index . . . . .	522
Memory Usage and the Paging File . . . . .	524
Processor Scheduling . . . . .	527
SuperFetch . . . . .	527
ReadyBoost and ReadyDrive . . . . .	528
Cram Quiz . . . . .	529
Cram Quiz Answers . . . . .	530
Review Questions . . . . .	531
Answers to Review Questions . . . . .	533

**CHAPTER 16:**

<b>Backups and System Recovery . . . . .</b>	<b>535</b>
Looking at Events . . . . .	536
Event Viewer . . . . .	537
Reliability Monitor . . . . .	541
Action Center . . . . .	542
System Information . . . . .	543
Diagnostic Tools . . . . .	544
Boot Tools . . . . .	546

System Recovery Disc . . . . .	551
Windows PE Disk . . . . .	553
Problem Steps Recorder. . . . .	554
Cram Quiz . . . . .	556
Cram Quiz Answers . . . . .	556
Backups and System Recovery. . . . .	558
Backup Overview . . . . .	559
Types of Backups . . . . .	560
Backup and Restore Center . . . . .	562
System Image Backup . . . . .	564
System Protection. . . . .	564
Cram Quiz . . . . .	568
Cram Quiz Answers . . . . .	568
Review Questions. . . . .	569
Review Question Answers . . . . .	571
<b>Practice Exam . . . . .</b>	<b>573</b>
<b>Index. . . . .</b>	<b>591</b>

# About the Author

**Patrick Regan** has been a PC technician, network administrator/engineer, design architect, and security analyst for the past 17 years since graduating with a bachelor's degree in physics from the University of Akron. He has taught many computer and network classes at Sacramento local colleges (Heald Colleges and MTI Colleges) and participated in and led many projects (Heald Colleges, Intel Corporation, Miles Consulting Corporation, and Pacific Coast Companies). For his teaching accomplishments, he received the Teacher of the Year award from Heald Colleges, and he has received several recognition awards from Intel. Previously, he worked as a product support engineer for the Intel Corporation Customer Service, a senior network engineer for Virtual Alert supporting the BioTerrorism Readiness suite and as a senior design architect/engineer and training coordinator for Miles Consulting Corporation (MCC), a premiere Microsoft Gold partner and consulting firm. He is currently a senior network engineer supporting a large enterprise network at Pacific Coast Companies.

He holds many certifications including the Microsoft MCSE, MCSA, MCT; CompTIA's A+, Network+, Server+, Linux+, Security+ and CTT+; Cisco CCNA; and Novell's CNE and CWNP Certified Wireless Network Administrator (CWNA).

Over the last several years, he has written several textbooks for Prentice Hall, including *Troubleshooting the PC*, *Networking with Windows 2000 and 2003*, *Linux*, *Local Area Networks*, *Wide Area Networks*, and the *Acing Series* (*Acing the A+*, *Acing the Network+*, *Acing the Security+*, and *Acing the Linux+*). He has also co-authored the *MCSA/MCSE 70-290 Exam Cram: Managing and Maintaining a Microsoft Windows Server 2003 Environment*, Second Edition and has written several *Exam Cram* books for the Windows Vista and Windows Server 2008 certification exams.

You can write with questions and comments to the author at [Patrick\\_Regan@hotmail.com](mailto:Patrick_Regan@hotmail.com). (Because of the high volume of mail, every message might not receive a reply.)

# Dedication

*I dedicate this book to the most beautiful woman and most wonderful person, Lidia.  
She is the best there is.*

## About the Technical Reviewer

**Christopher A. Crayton** is an author, technical editor, technical consultant, security consultant, trainer, and SkillsUSA state-level technology competition judge. Formerly, he worked as a computer and networking instructor at Keiser College (2001 Teacher of the Year); as network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak Headquarters as a computer and network specialist. Chris has authored several print and online books, including *The A+ Exams Guide*, Second Edition (Cengage Learning, 2008), *Microsoft Windows Vista 70-620 Exam Guide Short Cut* (O'Reilly, 2007), *CompTIA A+ Essentials 220-601 Exam Guide Short Cut* (O'Reilly, 2007), *The A+ Exams Guide*, *The A+ Certification and PC Repair Handbook* (Charles River Media, 2005), *The Security+ Exam Guide* (Charles River Media, 2003), and *A+ Adaptive Exams* (Charles River Media, 2002). He is also co-author of *How to Cheat at Securing Your Network* (Syngress, 2007). As an experienced technical editor, Chris has provided many technical edits/reviews for several major publishing companies, including Pearson Education, McGraw-Hill, Cengage Learning, Wiley, O'Reilly, Syngress, and Apress. He holds MCSE, A+, and Network+ certifications.



# We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.*

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: [feedback@pearsonitcertification.com](mailto:feedback@pearsonitcertification.com)

Mail: Dave Dusthimer  
Associate Publisher  
Pearson IT Certification  
800 East 96th Street  
Indianapolis, IN 46240 USA

## Reader Services

Visit our website and register this book at [www.pearsonitcertification.com/register](http://www.pearsonitcertification.com/register) for convenient access to any updates, downloads, or errata that might be available for this book.

# Introduction

Welcome to *MCTS 70-680 Exam Cram: Microsoft Windows 7, Configuring!* Whether this book is your first or your fifteenth *Exam Cram* series book, you'll find information here that will help ensure your success as you pursue knowledge, experience, and certification. This book aims to help you get ready to take and pass the Microsoft certification exam "TS: Windows 7, Configuring" (Exam 70-680). After you pass this exam, you will earn the Microsoft Certified Technology Specialist: Windows 7, Configuration certification.

This introduction explains Microsoft's certification programs in general and talks about how the *Exam Cram* series can help you prepare for Microsoft's latest certification exams. Chapters 1 through 16 are designed to remind you of everything you need to know to pass the 70-680 certification exam. At the beginning and end of each main section, you see Cram Saver and Cram Exam questions to review the material. Then, at the end of each chapter, you find 10 review questions, and at the end of the book, you find a practice exam. Read the book, understand the material, and you stand a very good chance of passing the real test.

Based on what you learn from the self-assessment, you might decide to begin your studies with classroom training or some background reading. On the other hand, you might decide to pick up and read one of the many study guides available from Microsoft or third-party vendors. We also recommend that you supplement your study program with visits to <http://examcram.com> to receive additional practice questions, get advice, and track the Windows certification programs.

## The Value of Certification

It is an established fact that computers and networking is a fast-paced environment. Therefore, employees who work in Information Technology (IT) must learn to keep up with the ever-changing technology and have the ability to learn new technology. It is said that a person in IT must be able to learn or retrain him- or herself every 1 to 1 1/2 years.

According to *Certification Magazine* (<http://www.certmag.com>), the successful IT worker must

- ▶ Be proficient in two or more technical specialties.
- ▶ Be able to wear multiple hats.
- ▶ Be more business-oriented because hiring managers look for employees who see the big picture of profit, loss, competitive advantage, and customer retention and understand that IT fits into this picture.
- ▶ Be able to work easily with non-technical personnel.
- ▶ Have soft skills of good listening, problem-solving, and effective written and verbal communication.

In addition, there is a demand for those who can demonstrate expertise in IT project management. Those moving to a mid- to high-level position have a mix of academic credentials and industry certifications, as well as increasing levels of responsibility.

Today, technical certifications are highly valuable. Depending on which certification or certifications an individual has, a user can begin as an entry-level technician or administrator. Certifications also demonstrate the knowledge and capabilities of a current technician or administrator. Technical companies see some technical certifications as valuable as a college degree and non-technical companies see them just a little less than a college degree.

In 2001, researchers from Gartner Consulting surveyed nearly 18,000 IT managers, certified professionals, and certification candidates. They reported that

- ▶ IT professionals seek certification to increase compensation, find employment, or boost productivity.
- ▶ Of those certified, 66% of certified professionals received an increase in salary after becoming certified, and 83% reported that certification helped them gain a new position.
- ▶ Although most certification candidates combine several study methods, printed materials designed for self-study and instructor-led training were reported as the most useful preparation methods.

From the employer's perspective, although many managers (42%) feared that certified employees would move on to another organization, 71% of IT professionals gaining certification stay put. IT managers cited a higher level of

service, competitive advantage, and increased productivity as key benefits of having certified staff. Of course, the drawbacks include cost of training and testing.

So as you can see, many people in IT see certification as a valuable tool. You can see that certification is

- ▶ A demonstration of specific areas of competence with particular technologies.
- ▶ A credential desired or required by an increasing number of employers.
- ▶ A tool people use successfully to challenge themselves.
- ▶ A road map for continuing education.
- ▶ A potential bridge to a new specialty.
- ▶ Evidence that you are self-motivated and actively working to stay current.

On the other hand, certification is not a substitute for extensive hands-on experience, and it is not a career cure-all. Lastly, usually a little bit of work and discipline is required to pass these exams.

## The Microsoft Certification Program

Microsoft currently offers multiple certification titles, each of which boasts its own special abbreviation. (As a certification candidate and computer professional, you need to have a high tolerance for acronyms.)

Certifications for end-users are

- ▶ **Microsoft Office Specialists:** Recognized for demonstrating advanced skills with Microsoft desktop software (including Microsoft Office).

The older certifications associated with the Windows Server 2003 operating system and related network infrastructure are as follows:

- ▶ **Microsoft Certified Professional (MCP):** For professionals who have the skills to successfully implement a Microsoft product (such as Windows XP or Windows Server 2003) or technology as part of a business solution in an organization.

- ▶ **Microsoft Certified Desktop Support Technician (MCDST):** For professionals who have the technical and customer service skills to troubleshoot hardware and software operation issues in Microsoft Windows environments.
- ▶ **Microsoft Certified Systems Administrators (MCSAs):** For professionals who administer network and systems environments based on the Microsoft Windows operating systems. Specializations include MCSA: Messaging and MCSA: Security.
- ▶ **Microsoft Certified Systems Engineer (MCSE):** For professionals who design and implement an infrastructure solution that is based on the Windows operating system and Microsoft Windows Server System software. Specializations include MCSE: Messaging and MCSE: Security.

The newer certification base on Windows Vista and related server products are

- ▶ **Microsoft Certified Technology Specialist (MCTS):** For professionals who target specific technologies and to distinguish themselves by demonstrating in-depth knowledge and expertise in the various Microsoft specialized technologies. The MCTS is a replacement for the MCP program.
- ▶ **Microsoft Certified IT Professional (MCITP):** For professionals who demonstrate comprehensive skills in planning, deploying, supporting, maintaining, and optimizing IT infrastructures. The MCITP is a replacement for the MCSA and MCSE programs.
- ▶ **Microsoft Certified Architect (MCA):** For professionals who are identified as top industry experts in IT architecture that use multiple technologies to solve business problems and provide business metrics and measurements. Candidates for the MCA program are required to present to a review board—consisting of previously certified architects—to earn the certification.

For database professionals:

- ▶ **Microsoft Certified Database Administrators (MCDDBAs):** For professionals who design, implement, and administer Microsoft SQL Server databases.

For developers and programmers:

- ▶ **Microsoft Certified Professional Developer (MCPD):** Professionals who are recognized as expert Windows Application Developer, Web Application Developer, or Enterprise Applications Developer. They demonstrate that you can build rich applications that target a variety of platforms, such as the Microsoft .NET Framework 2.0.
- ▶ **Microsoft Certified Application Developers (MCADs):** For professionals who use Microsoft technologies to develop and maintain department-level applications, components, Web or desktop clients, or back-end data services.

For trainers and curriculum developers, there is the

- ▶ **Microsoft Certified Trainer (MCT):** For qualified instructors who are certified by Microsoft to deliver Microsoft training courses to IT professionals and developers.
- ▶ **Microsoft Certified Learning Consultant (MCLC):** For recognized MCTs whose job roles have grown to include frequent consultative engagements with their customers and who are experts in delivering customized learning solutions that positively affect customer return on investment (ROI).

The best place to keep tabs on all Microsoft certifications is the following website:

<http://www.microsoft.com/learning/default.aspx>

Because Microsoft changes the website often and this URL might not work in the future, you should use the Search tool on Microsoft's site to find more information on a particular certification.

## Microsoft Certified Technology Specialist

Technology Specialist certifications enable professionals to target specific technologies and to distinguish themselves by demonstrating in-depth knowledge and expertise in their specialized technologies. Microsoft Technology Specialists are consistently capable of implementing, building, troubleshooting, and debugging a particular Microsoft technology.

## Microsoft Certified IT Professional

The new Microsoft Certified IT Professional (MCITP) credential lets you highlight your specific area of expertise. Now you can easily distinguish yourself as an expert in database administration, database development, business intelligence, or support. Some of the Microsoft Certified IT Professional certifications are

- ▶ IT Professional: Database Developer
- ▶ IT Professional: Database Administrator
- ▶ IT Professional: Business Intelligence Developer
- ▶ IT Professional: Enterprise Support Technician

At the time of this writing, details are just starting to be revealed on the Microsoft Certified Technology Specialist (MCTS) on Windows Server 2008/Windows Server 2008 R2. The MCTS on Windows Server 2008 helps you and your organization take advantage of advanced server technology with the power to increase the flexibility of your server infrastructure, save time, and reduce costs. Transition certifications are available today for Windows Server 2003 certified professionals to Windows Server 2008 Windows Server 2008 R2 product release. For more details about these certifications, visit the following website:

<http://www.microsoft.com/learning/mcp/windowsserver2008/default.mspx>

If the URL is no longer available, don't forget to search for MCTS and Windows Server 2008 using the Microsoft search tool found on the Microsoft website.

## Microsoft Certified Technology Specialist: Windows 7 Configuration

The Microsoft Certified Technology Specialist certifications enable professionals to target specific technologies and distinguish themselves by demonstrating in-depth knowledge and expertise in their specialized technologies. A

Microsoft Certified Technology Specialist in Windows 7, Configuration possesses the knowledge and skills to configure Windows 7 for optimal performance on the desktop, including installing, managing, and configuring the new security, network, and application features in Windows 7.

To earn the Microsoft Certified Technology Specialist: Windows 7, Configuration, you must pass one exam that focuses on supporting end-user issues about network connectivity, security, and applications installation and compatibility, and logon problems that include account issues and password resets:

Exam 70-680 TS: Windows 7, Configuration

If you decide to take Microsoft recognized class, you would take several classes to cover all of the material found on this exam. The preparation guide (including exam objectives) for Exam 70-680 TS: Windows 7, Configuration can be found at

<http://tinyurl.com/ye8mjce>

Table I.1 outlines the major topic areas, individual exam objectives, and which chapters in the book cover these objectives.

TABLE I.1 **MCTS 70-680 Exam Outline**

Exam Topic Area (Percentage of Exam)	Exam Objective	Exam Objective Description	Chapter Covering Exam Objective
<b>Installing, Upgrading, and Migrating to Windows 7 (14 percent)</b>	Perform a clean installation	This objective might include but is not limited to identifying hardware requirements; setting up as the sole operating system; setting up as dual boot; installation methods; boot from the source of installation, preparing the installation source: USB, CD, network share, WDS.	Chapter 2
	Upgrade to Windows 7 from previous versions of Windows	This objective might include but is not limited to upgrading from Windows Vista; migrating from Windows XP; upgrading from one edition of Windows 7 to another edition of Windows 7.	Chapter 2



TABLE I.1 **Continued**

<b>Exam Topic Area (Percentage of Exam)</b>	<b>Exam Objective</b>	<b>Exam Objective Description</b>	<b>Chapter Covering Exam Objective</b>
	Migrate user profiles	This objective might include but is not limited to migrating from one machine to another; migrating from previous versions of Windows; side-by-side versus. wipe and load.	Chapter 2
<b>Deploying Windows 7 (13 percent)</b>	Capture a system image	This objective might include but is not limited to preparing system for capture; creating a WIM file; automated capture; manual capture.	Chapter 2
	Prepare a system image for deployment	This objective might include but is not limited to inserting an application into a system image; inserting a driver into a system image; inserting an update into a system image; configuring tasks to run after deployment.	Chapter 2
	Deploy a system image	This objective might include but is not limited to automated deployment methods; manually deploying a customized image.	Chapter 2
	Configure a VHD	This objective might include but is not limited to creating, deploying, booting, mounting, and updating VHDs; offline updates; offline servicing.	Chapter 2
<b>Configuring Hardware and Applications (14 percent)</b>	Configure devices	This objective might include but is not limited to updating, disabling, and uninstalling drivers; signed drivers; conflicts between drivers; configuring driver settings; resolving problem device drivers.	Chapter 3

TABLE I.1 **Continued**

<b>Exam Topic Area (Percentage of Exam)</b>	<b>Exam Objective</b>	<b>Exam Objective Description</b>	<b>Chapter Covering Exam Objective</b>
	Configure application compatibility	This objective might include but is not limited to setting compatibility mode; implementing shims; compatibility issues with Internet Explorer.	Chapters 12 and 13
	Configure application restrictions	This objective might include but is not limited to setting software restriction policies; setting application control policies; setting through group policy or local security policy.	Chapter 12
	Configure Internet Explorer	This objective might include but is not limited to configuring compatibility view; configuring security settings; configuring providers; managing add-ons; controlling InPrivate mode; certificates for secure websites.	Chapter 13
<b>Configuring Network Connectivity (14 percent)</b>	Configure IPv4 network settings	This objective might include but is not limited to connecting to a network; configuring name resolution; setting up a connection for a network; network locations; resolving connectivity issues; APIPA.	Chapter 5
	Configure IPv6 network settings	This objective might include but is not limited to configuring name resolution; connecting to a network; setting up a connection for a network; network locations; resolving connectivity issues; link local multicast name resolution.	Chapter 5

TABLE I.1 **Continued**

<b>Exam Topic Area (Percentage of Exam)</b>	<b>Exam Objective</b>	<b>Exam Objective Description</b>	<b>Chapter Covering Exam Objective</b>
	Configure networking settings	This objective might include but is not limited to adding a physically connected (wired) or wireless device; connecting to a wireless network; configuring security settings on the client; setting preferred wireless networks; configuring network adapters; configuring location-aware printing.	Chapters 5 and 6
	Configure Windows Firewall	This objective might include but is not limited to configuring rules for multiple profiles; allowing or denying an application; network-profile-specific rules; configuring notifications; configuring authenticated exceptions.	Chapter 7
	Configure remote management	This objective might include but is not limited to remote management methods; configuring remote management tools; executing PowerShell commands.	Chapter 14
<b>Configuring Access to Resources (13 percent)</b>	Configure shared resources	This objective might include but is not limited to folder virtualization; shared folder permissions; printers and queues; configuring Homegroup settings.	Chapters 10 and 11
	Configure file and folder access.	This objective might include but is not limited to encrypting files and folders by using EFS; configuring NTFS permissions; resolving effective permissions issues; copying files versus moving files.	Chapters 9 and 10

TABLE I.1 **Continued**

<b>Exam Topic Area (Percentage of Exam)</b>	<b>Exam Objective</b>	<b>Exam Objective Description</b>	<b>Chapter Covering Exam Objective</b>
	Configure user account control (UAC)	This objective might include but is not limited to configuring local security policy; configuring admin versus standard UAC prompt behaviors; configuring Secure Desktop.	Chapter 8
	Configure authentication and authorization	This objective might include but is not limited to resolving authentication issues; configuring rights; managing credentials; managing certificates; smart cards with PIV; elevating user privileges; multifactor authentication.	Chapter 8
	Configure BranchCache	This objective might include but is not limited to distributed cache mode versus hosted mode; network infrastructure requirements; configuring settings; certificate management.	Chapter 10
<b>Configuring Mobile Computing (10 percent)</b>	Configure BitLocker and BitLocker To Go	This objective might include but is not limited to configuring BitLocker and BitLocker To Go policies; managing Trusted Platform Module (TPM) PINs; configuring startup key storage; data recovery agent support.	Chapter 9
	Configure DirectAccess	This objective might include but is not limited to configuring client side; configuring authentication; network infrastructure requirements.	Chapter 6

TABLE I.1 **Continued**

<b>Exam Topic Area (Percentage of Exam)</b>	<b>Exam Objective</b>	<b>Exam Objective Description</b>	<b>Chapter Covering Exam Objective</b>
	Configure mobility options	This objective might include but is not limited to configuring offline file policies; transparent caching; creating and migrating power policy.	Chapter 14
	Configure remote connections	This objective might include but is not limited to establishing VPN connections and authentication; enabling a VPN reconnect; advanced security auditing; NAP quarantine remediation; dial-up connections; remote desktop; published apps.	Chapters 6, 8, and 14
<b>Monitoring and Maintaining Systems That Run Windows 7 (11 percent)</b>	Configure updates to Windows 7	This objective might include but is not limited to configuring update settings; determining source of updates; configuring Windows Update policies; reviewing update history; checking for new updates; rolling back updates.	Chapter 2
	Manage disks	This objective might include but is not limited to managing disk volumes; managing file system fragmentation; RAID; removable device policies.	Chapter 4
	Monitor systems	This objective might include but is not limited to configuring event logging; filtering event logs; event subscriptions; data collector sets; generating a system diagnostics report.	Chapters 15 and 16

TABLE I.1 **Continued**

<b>Exam Topic Area (Percentage of Exam)</b>	<b>Exam Objective</b>	<b>Exam Objective Description</b>	<b>Chapter Covering Exam Objective</b>
	Configure performance settings	This objective might include but is not limited to configuring page files; configuring hard drive cache; updated drivers; configuring networking performance; configuring power plans; configuring processor scheduling; configuring desktop environment; configuring services and programs to resolve performance issues; mobile computing performance issues; configuring power.	Chapter 15
<b>Configuring Backup and Recovery Options (11 percent)</b>	Configure backup	This objective might include but is not limited to creating a system recovery disk; backing up files, folders, or full system; scheduling backups.	Chapter 16
	Configure system recovery options	This objective might include but is not limited to configuring system restore points; restoring system settings; last known good configuration; complete restore; driver rollback.	Chapters 3 and 16
	Configure file recovery options	This objective might include but is not limited to configuring file restore points; restoring previous versions of files and folders; restoring damaged or deleted files by using shadow copies; restoring user profiles.	Chapter 16

# Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take Exam 70-680 is (U.S.) \$125, and if you don't pass, you can take each again for an additional (U.S.) \$125 for each attempt. In the United States and Canada, tests are administered by Prometric. Here's how you can contact them:

- ▶ **Prometric:** You can sign up for a test through the company's website, <http://www.2test.com> or <http://www.prometric.com>. Within the United States and Canada, you can register by phone at 800-755-3926. If you live outside this region, you should check the Prometric website for the appropriate phone number.

To sign up for a test, you must possess a valid credit card or contact either Prometric for mailing instructions to send a check (in the U.S.). Only when payment is verified, or a check has cleared, can you actually register for a test.

To schedule an exam, you need to call the appropriate phone number or visit the Prometric websites at least one day in advance of the test date. To cancel or reschedule an exam in the United States or Canada, you must call before 3 p.m. Eastern time the day before the scheduled test time (or you might be charged, even if you don't show up to take the test). When you want to schedule a test, you should have the following information ready:

- ▶ Your name, organization, and mailing address.
- ▶ Your Microsoft test ID. (In the United States, this means your Social Security number; citizens of other countries should call ahead to find out what type of identification number is required to register for a test.)
- ▶ The name and number of the exam you want to take.
- ▶ A method of payment. (As mentioned previously, a credit card is the most convenient method, but alternate means can be arranged in advance, if necessary.)

After you sign up for a test, you are told when and where the test is scheduled. You should arrive at least 15 minutes early. You must supply two forms of identification, one of which must be a photo ID, to be admitted into the testing room.

# How to Prepare for an Exam

Preparing for any Microsoft certification test (including Exam 70-680) requires that you obtain and study materials designed to provide comprehensive information about the product and its capabilities that will appear on the specific exam for which you are preparing. The following list of materials can help you study and prepare:

- ▶ The Windows 7 product DVD-ROM. This disk includes comprehensive online documentation and related materials; it should be one of your primary resources when you are preparing for the test. Currently, you can download a Windows 7 Enterprise 90-day trial from the following website:  
<http://technet.microsoft.com/en-us/evalcenter/cc442495.aspx>
- ▶ The exam preparation materials, practice tests, and self-assessment exams on the Microsoft Training and Certification site, at <http://www.microsoft.com/learning/default.msp>. The Exam Resources link offers samples of the new question types on the Windows Server 2003/2008 Microsoft Certification track series of exams. You should find the materials, download them, and use them!
- ▶ The exam preparation advice, practice tests, questions of the day, and forums at <http://www.examcram.com>.

In addition, you might find any or all of the following materials useful in your quest for Windows 7 expertise:

- ▶ **Microsoft training kits:** Microsoft Learning offers a training kit that specifically targets Exam 70-680. For more information, visit <http://www.microsoft.com/learning/books/>. This training kit contains information that you will find useful in preparing for the test.
- ▶ **Microsoft TechNet CD or DVD and website:** This monthly CD- or DVD-based publication delivers numerous electronic titles that include coverage of Windows Server 2003 and Windows Server 2008 and related topics on the Technical Information (TechNet) series on CD or DVD. Its offerings include product facts, technical notes, tools and utilities, and information on how to access the Seminars Online training materials for Windows Server 2003/2008 and the Windows Server System line of products. Visit <http://technet.microsoft.com> and check out the information for TechNet subscriptions. You can utilize a large portion of the TechNet website at no charge.



- ▶ **Study guides:** Several publishers—including Pearson—offer Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, and Windows XP study guides. Pearson offers the following:
  - ▶ **The Exam Cram series:** These books give you the insights about the material that you need to know to successfully pass the certification tests.
  - ▶ **Pearson Certification Guides:** These books provide a greater level of detail than the *Exam Cram* books and are designed to teach you everything you need to know about the subject covered by an exam. Each book comes with a CD-ROM that contains interactive practice exams in a variety of testing formats.

Together, these two series make a perfect pair if you are new to Windows.

- ▶ **Classroom training:** CTECs, online partners, and third-party training companies (such as Wave Technologies, New Horizons, and Global Knowledge) offer classroom training on Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, and Windows XP. These companies aim to help you prepare to pass Exam 70-680 as well as several others. Although this type of training tends to be pricey, most of the individuals lucky enough to attend find this training to be quite worthwhile.

Although many websites offer information on what to study for a particular exam, few sites offer how you should study for an exam. The study process can be broken down into various stages. However, key to all of these stages is the ability to concentrate. Concentration, or the lack of, plays a big part in the study process.

To be able to concentrate, you must remove all distractions. You should plan for study breaks, but it is the unplanned breaks caused by distractions that do not allow you to concentrate on what you need to learn. Therefore, first, you need to create an environment that's conducive to studying or seek out an existing environment that meets these criteria, such as a library.

First, do not study with the TV on and do not have other people in the room. It is easy for the TV to break your concentration and grab your attention. In addition, if you have people in the room, you have to pretend that you are not there and that they are not causing distractions, including talking with other people. Lastly, there are varying opinions on whether it is better to study with

or without music playing. Although some people need to have a little white noise in the background to study, if you do choose to have music, you should keep the volume on a low level and you should listen to music without vocals in it.

After you find a place to study, you must schedule the time to study. You should take into consideration not studying on an empty stomach. You should also not study on a full stomach because it tends to make people drowsy. You might also consider having a glass of water near to sip on.

In addition, make sure that you well rested so that you don't start dozing off when you start. Next, make sure that you find a position that is comfortable and that the furniture that you are using is also comfortable. Lastly, make sure that your study area is well lit. Natural light is best for fighting fatigue.

The first thing that you should do when you study is to clear your mind of distractions. So take a minute or two, close your eyes, and empty your mind.

When you prepare for an exam, the best place to start is to take the list of exam objectives and study them carefully. You can then organize your study keeping these objectives in mind. This narrows down your focus area to individual topics or subtopics. In addition, you need to understand and visualize the process as a whole. This helps in addressing practical problems in real environments as well as some unsuspected questions.

In a multiple-choice type exam, you do have one advantage: The answer or answers are already there, and you have to simply choose the correct ones. Because the answers are already there, you can start eliminating the incorrect answers by using your knowledge and some logical thinking. One common mistake is to select the first obvious-looking answers without checking the other options, so always examine all the options, think, and choose the right answer. Of course, with multiple-choice questions, you have to be exact and should be able to differentiate between very similar answers. This is where a peaceful place of study without distractions helps so that you can read between the lines and so that you don't miss key points.

## **Day of the Exam**

Before you take an exam, eat something light, even if you have no appetite. If your stomach is actively upset, try mild foods such as toast or crackers. Plain saltine crackers are great for settling a cranky stomach. Keep your caffeine and nicotine consumption to a minimum; excessive stimulants aren't exactly

conducive to reducing stress. Plan to take a bottle of water or some hard candies, such as lozenges, with you to combat dry mouth. Also, make sure to dress comfortably.

Arrive at the testing center early. If you have never been to the testing center before, make sure that you know where it is. You might even consider taking a test drive. If you arrive between 15 and 30 minutes early for any certification exam, it gives you

- ▶ Ample time for prayer, meditation, and/or breathing.
- ▶ Time to scan glossary terms and quick access tables before taking the exam so that you can get the intellectual juices flowing and build a little confidence.
- ▶ Time to practice physical relaxation techniques.
- ▶ Time to visit the washroom.

But don't arrive too early.

When you are escorted into the testing chamber, you are usually given two sheets of paper (or laminated paper) with a pen (or wet erase pen). As soon as you hear the door close behind you, immediately unload bits of exam information that you need to quickly recall onto the paper. Then throughout the exam, you can refer to this information easily without thinking about it. This way, you can focus on answering the questions and using this information as reference. Before you actually start the exam, close your eyes and take deep breath to clear your mind of distractions.

Typically, the testing room is furnished with anywhere from one to six computers, and each workstation is separated from the others by dividers designed to keep anyone from seeing what's happening on someone else's computer screen. Most testing rooms feature a wall with a large picture window. This layout permits the exam coordinator to monitor the room, to prevent exam takers from talking to one another, and to observe anything out of the ordinary that might go on. The exam coordinator will have preloaded the appropriate Microsoft certification exam—for this book, that's Exam 70-680 MCTS: Windows 7, Configuring—and you are permitted to start as soon as you're seated in front of the computer.

**ExamAlert**

Always remember that the testing center's test coordinator is there to assist you in case you encounter some unusual problems, such as a malfunctioning test computer. If you need some assistance not related to the content of the exam itself, feel free to notify one of the test coordinators—after all, they are there to make your exam-taking experience as pleasant as possible.

All exams are completely closed book. In fact, you are not permitted to take anything with you into the testing area, but you receive a blank sheet of paper and a pen or, in some cases, an erasable plastic sheet and an erasable pen. We suggest that you immediately write down on that sheet of paper all the information you've memorized for the test. In *Exam Cram* books, this information appears on the tear-out sheet (Cram Sheet) inside the front cover of each book. You are given some time to compose yourself, record this information, and take a sample orientation exam before you begin the real thing. We suggest that you take the orientation test before taking your first exam, but because all the certification exams are more or less identical in layout, behavior, and controls, you probably don't need to do so more than once.

All Microsoft certification exams allow a certain maximum amount of testing time. (This time is indicated on the exam by an onscreen timer clock, so you can check the time remaining whenever you like.) All Microsoft certification exams are computer generated. In addition to multiple choice, most exams contain select-and-place (drag-and-drop), create-a-tree (categorization and prioritization), drag-and-connect, and build-list-and-reorder (list prioritization) types of questions. Although this format might sound quite simple, the questions are constructed not only to check your mastery of basic facts and figures about Windows Vista, but also to require you to evaluate one or more sets of circumstances or requirements. Often, you are asked to give more than one answer to a question. Likewise, you might be asked to select the best or most effective solution to a problem from a range of choices—all of which are technically correct. Taking the exam is quite an adventure, and it involves real thinking and concentration. This book shows you what to expect and how to deal with the potential problems, puzzles, and predicaments.

## Dealing with Test Anxiety

Because a certification exam costs money to take and time to prepare for the exam and failing an exam can be a blow to your self-confidence, most people feel a certain amount of anxiety when they are about to take a certification exam. It is no wonder that most of us are a little sweaty in the palms when taking the exam. However, certain levels of stress can actually help you to raise your level of performance when taking an exam. This anxiety usually serves to help you focus your concentration and think clearly through a problem.

But for some individuals, exam anxiety is more than just a nuisance. For these people, exam anxiety is a debilitating condition that affects their performance with a negative impact on the exam results.

Exam anxiety reduction begins with the preparation process. The first thing that you should think of is if you know the material, there should not be anything that you should be nervous over. It goes without saying that the better prepared you are for an exam, the less stress you will experience when taking it. Always give yourself plenty of time to prepare for an exam; don't place yourself under unreasonable deadlines. But again, make goals and make every effort to meet those goals. Procrastination and making excuses can be just as bad.

There is not hard and fast rule for how long it takes to prepare for an exam. The time required varies from student to student and is dependent on a number of different factors including reading speed, access to study materials, personal commitments, and so on. In addition, don't compare yourself to peers, especially if doing so has a negative effect on your confidence.

For many students, practice exams are a great way to shed some of the fears that arise in the test center. Practice exams are best used near the end of the exam preparation. Be sure to use them as an assessment of your current knowledge, not as a method to try to memorize key concepts. When reviewing these questions, be sure you understand the question and understand all answers (right and wrong). Lastly, set time limits on the practice exams.

If you know the material, don't plan on studying the day of your exam. You should end your studying the evening before the exam. In addition, don't make it a late night so that you can get a full good night's rest. Of course, you should be studying on a regular basis for at least a few weeks prior to the evening of the exam so that you should not need the last-minute cramming.

# Additional Resources

A good source of information about Microsoft certification exams comes from Microsoft itself. Because its products and technologies—and the exams that go with them—change frequently, the best place to go for exam-related information is online.

Microsoft offers training, certification, and other learning-related information and links at the <http://www.microsoft.com/learning> web address. If you haven't already visited the Microsoft Training and Certification website, you should do so right now. Microsoft's Training and Certification home page resides at <http://www.microsoft.com/learning/default.aspx>.

---

## Coping with Change on the Web

Sooner or later, all the information we've shared with you about the Microsoft Certified Professional pages and the other Web-based resources mentioned throughout the rest of this book will go stale or be replaced by newer information. In some cases, the URLs you find here might lead you to their replacements; in other cases, the URLs will go nowhere, leaving you with the dreaded "404 File not found" error message. When that happens, don't give up.

There's always a way to find what you want on the Web if you're willing to invest some time and energy. Most large or complex websites—and Microsoft's qualifies on both counts—offer search engines. All of Microsoft's web pages have a Search button at the top edge of the page. As long as you can get to Microsoft's site (it should stay at <http://www.microsoft.com> for a long time), you can use the Search button to find what you need.

The more focused (or specific) you can make a search request, the more likely the results will include information you can use. For example, you can search for the string

`"training and certification"`

to produce a lot of data about the subject in general, but if you're looking for the preparation guide for Exam 70-680: Windows 7, Configuring, you'll be more likely to get there quickly if you use a search string similar to the following:

`"Exam 70-680" AND "preparation guide"`

Likewise, if you want to find the Training and Certification downloads, you should try a search string such as this:

`"training and certification" AND "download page"`

Finally, you should feel free to use general search tools—such as <http://www.google.com>, <http://www.yahoo.com>, <http://www.excite.com>, and <http://www.bing.com>—to look for related information. Although Microsoft offers great information about its certification exams online, there are plenty of third-party sources of information and assistance that need not follow Microsoft's party line. Therefore, if you can't find something where the book says it lives, you should intensify your search.

---

Thanks for making this *Exam Cram* book a pivotal part of your certification study plan. Best of luck on becoming certified!

## CHAPTER 1

# Introduction to Windows 7

### **This chapter covers the following 70-680 Objectives:**

- ▶ **Supplemental Objective:** List and describe the main differences between Windows 7, Windows Vista, and Windows XP.
- ▶ **Supplemental Objective:** List the different editions of Windows 7.
- ▶ **Supplemental Objective:** Describe the difference between the 32-bit and 64-bit versions of Windows 7.
- ▶ **Supplemental Objectives:** List and describe the main components that make up the graphical user interface used in Windows 7.

Before discussing the exact objectives found in the 70-680 exam, you need to understand how Windows 7 came about and what is different between Windows 7 and older versions of Windows, specifically Windows XP and Windows Vista. Before you decide to install Windows 7, you need to know which editions and versions are available so that you can choose the correct version for you.

Furthermore, if you are new to Windows 7, you will notice the Windows graphical user interface is significantly different than Windows XP and, to a lesser degree, Windows Vista. So before you jump into the “blood and guts” of Windows 7, make sure that you understand the basics of using Windows 7.



# The Road to Windows 7

- ▶ **Supplemental Objective:** List and describe the main differences between Windows 7, Windows Vista, and Windows XP.
- ▶ **Supplemental Objective:** List the different editions of Windows 7.
- ▶ **Supplemental Objective:** Describe the difference between the 32-bit and 64-bit versions of Windows 7.

## CramSaver

1. Which edition of Windows 7 is aimed at large corporations and includes numerous tools to secure Windows, including BitLocker and AppLocker?
  - A. Windows 7 Home Premium
  - B. Windows 7 Professional
  - C. Windows 7 Enterprise
  - D. Windows 7 Ultimate
  
2. You want to access 64 GB of memory. Which edition of Windows 7 should you use?
  - A. 16 MB
  - B. 32-bit
  - C. 32 GB
  - D. 64-bit
  - E. 64 GB

## Answers

1. **C** is correct. Windows 7 Enterprise provides advanced data protection and information access for businesses. It is targeted for managed environments, mainly large enterprises. It includes BitLocker, BitLocker To Go, AppLocker, Direct Access, and BranchCache. Answer A is incorrect because Windows 7 Home Premium is aimed at home consumers. Answer B is incorrect because Windows 7 Professional is the business-focused edition for small and lower mid-market companies. It does not include BitLocker and AppLocker. Answer D is incorrect because although Windows 7 Ultimate has all the components that Windows 7 Enterprise has, it has additional features that are not needed for an Enterprise environment.
2. **D** is correct. Windows 7 comes in two flavors, 32-bit and 64-bit. If you want to recognize more than 4 GB of memory, you need to use the 64-bit version. Answer B is incorrect because 32-bit Windows only supports up to 4 GB of memory. Answers A, C, and E are incorrect because the 16 MB, 32 GB, and 64 GB editions do not exist.

Windows XP was first released on October 25, 2001. Windows XP grew to be the most widely used operating system, which peaked in December 2006 with more than 400 million copies and an 85.3% market share. Even after the release of Windows Vista, as of July 2010, Windows XP still remains the most widely used operating system with a 54.6% market share. Compared to previous versions of Windows, Windows XP was known for its improved functionality, stability, and flexibility while providing an easy-to-use interface. As a result, Windows XP became the de facto standard for the desktop and laptop operating systems for corporations around the world.

Windows XP was aimed at both the corporate and consumer world. The most common editions of the operating system are Windows XP Home Edition, which was aimed at home users, and Windows XP Professional Edition, which was targeted at power users and corporate clients.

The more popular versions of Windows before Windows XP were partially based on DOS, which was the base operating system that worked underneath Windows. To finally break the limitations imposed by DOS, Windows XP was built on the Windows NT architecture instead of using DOS as a base OS. Although Windows XP could run a DOS virtual machine to run DOS applications, it did not allow DOS programs to communicate directly with the hardware without going through Windows (this is necessary to keep the system secure). As a result, some DOS programs would not operate under Windows XP. Nonetheless, Windows XP ushered in Windows for the masses at home and in the corporate office.

One of the biggest criticisms of Windows XP has been security. The design of Windows XP placed some emphasis on security; however, the security features were not the highest priority. Because Windows XP became the de facto standard for operating systems, it became a popular platform to attack by hackers and programmers who looked for and exploited weaknesses within the operating system, usually using malware such as viruses, Trojan horses, and worms. As a result, Microsoft has released numerous security patches and three service packs to help make Windows XP more secure. In addition, it is highly recommended that your system includes an up-to-date antivirus program that includes anti-spyware software and that the system is protected with some form of firewall. In fact, Windows XP Service Packs 2 and 3 include the Windows Firewall to help make Windows more secure.

Windows XP was such a success that the next major release of Windows did not occur for five years. On January 30, 2007, Windows Vista was released worldwide. Unfortunately, Windows Vista received an overall negative reception based on numerous reasons, including

- ▶ Confusion over hardware requirements and higher hardware requirements to utilize all features available from Windows Vista, including the new Windows Aero interface, while maintaining decent performance.
- ▶ Annoying security features, such as User Account Control, that generated too many prompts for you to proceed with common actions.
- ▶ A new interface that makes it more difficult for corporations to transition to the new version of Windows because of the involved learning curve and the increase in support calls.
- ▶ Expensive licenses compared to Windows XP and additional cost for corporations who already had an investment in Windows XP and saw no real benefit for paying significant amounts of money to upgrade to Windows Vista.
- ▶ Although every new operating system has compatibility problems with older applications, Windows Vista had more than its share of popular applications that would not operate under Windows Vista or ran poorly even if using application-compatible settings.
- ▶ Hardware incompatibility caused by changes in the driver models and requiring 64-bit versions of Windows Vista, allowing only signed drivers to be installed in kernel mode. This caused many hardware devices not to run under Windows Vista or to run very poorly.
- ▶ Poor game quality and game performance.
- ▶ Overall slower performance.
- ▶ Software bloat.
- ▶ Poor laptop battery life.

Although Microsoft tried to address some of the complaints with Service Pack 1, Windows Vista was not widely accepted. Many people purchased Windows Vista only to use the downgrade license to run Windows XP, particularly within corporations.

After a rocky run for Windows Vista, Microsoft tried to address the concerns of Windows Vista by releasing Windows 7. Although Windows 7 is based on the Windows Vista core, there are many improvements and enhancements, including

- ▶ Improved thicker taskbar with improved Notification Area and integrated quick launch/application pinning capability and improved taskbar previews.

- ▶ Enhanced desktop, including bigger icons and peek-into-desktop features.
- ▶ Removal of sidebar and integration of gadgets into the desktop.
- ▶ Jump Lists that enable speedy access to your favorite pictures, songs, websites, and documents.
- ▶ Internet Explorer 8, Windows Media Player 12, and DirectX 11.
- ▶ Reduced memory thumbprint and reduced I/O reads.
- ▶ Enhanced power management capabilities.
- ▶ Improved User Access Control (UAC), including fewer prompts and enhanced granularity of notifications.
- ▶ Improved mobile device support, including new power-saving features.
- ▶ Easier wireless networking.
- ▶ Simplified configuration of home networks using HomeGroup.
- ▶ Use of libraries to replace the old documents, pictures, and similar folders.
- ▶ Windows XP mode that enables you to run older Windows XP business software on your Windows 7 desktop using virtual technology.
- ▶ Capability to natively mount Virtual Hard Disk (VHD) files using the diskpart tool and the capability to run Windows 7 from a VHD file.
- ▶ DirectAccess that gives mobile users seamless access to corporate networks without a need to establish a virtual private network (VPN) connection.
- ▶ BranchCache decreases the time branch office users spend waiting to download files across the network.

Because Windows 7 is built on the Windows Vista core, the application and driver compatibility issues should be kept to a minimum.

## Defining Windows 7

Windows 7 is the latest version (following Windows XP and Vista) of Microsoft Windows operating system produced by Microsoft for use on personal computers, including home and business desktops, laptops, netbooks, tablet PCs, and media center PCs. It was released to manufacturers on July 22, 2009 and to the general public on October 22, 2009.

Windows 7 is called 7 because it is based on the seventh version of the Windows Kernel. Table 1.1 outlines the popular versions of Windows based on the Windows NT kernel.

TABLE 1.1 **Windows Versions**

Windows Operating System	Windows Kernel Version	Date of Release
Windows NT 4.0	4.0	1996
Windows 2000	5.0	2000
Windows XP	5.1	2001
Windows Vista	6.0	2007
Windows 7	7.0	2009

As an operating system, Windows 7 enables you to coordinate hardware and software and enables you to run business/productivity and entertainment applications. It also enables you to save and access data usually stored in documents or other data files.

Windows 7 includes many features that enable users to be more productive while providing an easy-to-use interface. It also provides a more secure desktop environment and a higher level of reliability when compared to the previous versions of Windows.

For more information about Windows 7, visit the following website:

<http://www.microsoft.com/windows/windows-7/default.aspx>

For more information comparing Windows XP, Windows Vista, and Windows 7, visit the following website:

<http://www.microsoft.com/windows/windows-7/compare/versions.aspx>

## Windows 7 Flavors

Similar to Windows Vista, Windows 7 is available in many flavors, including six Windows 7 editions and two platforms (32-bit and 64-bit). You should choose the edition and platform based on your current hardware and the desired functionality.

## Editions of Windows 7

There are six Windows 7 editions: two editions for mainstream consumers and business users and four specialized editions for enterprise customers,

technical enthusiasts, emerging markets, and entry-level PCs. They include the following:

- ▶ **Windows 7 Starter:** This edition is targeted specifically for small form factor PCs (such as cubes and book-size PCs) in all markets. It is only available for 32-bit platforms. It includes an improved Windows taskbar and Jump Lists, Windows Search, ability to join a HomeGroup, Action Center, Device Stage, Windows Fax and Scan, and enhanced media streaming. Initially when Windows 7 Starter was released, it was limited to run three applications at the same time. Microsoft has since removed this restriction and runs as many applications as the hardware can handle.
- ▶ **Windows 7 Home Basic:** This edition is targeted for value PCs in emerging markets and is meant for accessing the Internet and running basic productivity applications. It includes all features available in Windows 7 Starter, and other features, such as Live Thumbnail previews, enhanced visual experiences, and advanced networking support. It lacks most Aero support, has limited networking capabilities, and does not include the Windows Media Center application.
- ▶ **Windows 7 Home Premium:** This edition is the standard edition for customers. It provides full functionality on the latest hardware, easy ways to connect, and a visually rich environment. This edition includes all features available in Windows 7 Home Basic and other features, such as Windows Aero, Windows Touch, ability to create a HomeGroup, DVD Video playback and authoring, Windows Media Center, Snipping Tool, Sticky Notes, Windows Journal, and Windows SideShow.
- ▶ **Windows 7 Professional:** This edition is the business-focused edition for small and lower mid-market companies and users who have networking, backup, and security needs and multiple PCs or servers. It includes all features available in Windows 7 Home Premium, and other features, such as core business features including Domain Join and Group Policy, data protection with advanced network backup and Encrypted File System, ability to print to the correct printer at home or work with Location Aware Printing, Remote Desktop host, and Offline folders.
- ▶ **Windows 7 Enterprise:** This edition provides advanced data protection and information access for businesses. It is targeted for managed environments, mainly large enterprises. This edition includes all features available in Windows 7 Professional, and other features, such as BitLocker, BitLocker To Go, AppLocker, DirectAccess, BranchCache, Enterprise Search Scopes, all worldwide interface languages, Virtual Desktop Infrastructure (VDI) enhancements, and the ability to boot from a VHD.

- ▶ **Windows 7 Ultimate:** This edition is targeted for technical enthusiasts who want all Windows 7 features without a Volume License agreement. It includes all of the same features as the Windows 7 Enterprise. Windows 7 Ultimate is not licensed for VDI scenarios.

### ExamAlert

Be sure you know what features are available for each edition of Windows 7 so that you can choose the correct edition of Windows 7 if given a scenario.

Microsoft also produces an N edition of Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Professional, mostly aimed at the European market. The N editions of Windows 7 include all of the features as the corresponding editions, but the N editions do not include Microsoft Windows Media Player and related technologies. This enables you to install your own media player and associated components.

For more information about the Windows 7 Editions, visit the following websites:

<http://www.microsoft.com/windows/windows-7/compare/default.aspx>

[http://www.winsupersite.com/win7/win7\\_skus\\_compare.asp](http://www.winsupersite.com/win7/win7_skus_compare.asp)

## 32-Bit Versus 64-Bit

A 64-bit processor is a processor with a default word size of 64 bits and a 64-bit external data bus. Most people don't realize that today's processors can already handle 64-bit calculations. But one of the main benefits of 64-bit processors is that they can process significantly more memory than 32-bit processors (4 GB with a 32-bit address bus and 64 GB with a 36-bit address bus). Windows 7 Home Premium edition can recognize up to 16 GB of RAM, and Windows 7 Enterprise and Windows 7 Ultimate editions can recognize up to 192 GB. With more data in memory, a 64-bit processor can work faster because it doesn't have to swap large sets of information in and out of memory the way a 32-bit processor does. Today, just about every computer processor sold is a 64-bit processor.

If an operating system and programs are written to use the larger 64-bit calculations and to use the additional memory, the processing power of a computer can be significantly increased. Most programs designed for a computer running a 32-bit version of Windows work on a computer running 64-bit versions of

Windows. Notable exceptions are many antivirus programs and some hardware drivers. The biggest problem that you might encounter is finding 64-bit drivers for some of your older hardware devices because all drivers must also be 64-bit.

Note two things when using 64-bit Windows 7. You are not able to run legacy 16-bit applications unless you run them under a virtual environment such as XP Mode. Instead, you need to install XP mode to put an instance of x86 Windows XP SP3 on your x64 Windows 7 desktop and run the application from there. In addition, some 32-bit applications might run slightly slower.

### Note

IA-32 (Intel Architecture, 32-bit) was the de facto standard for Intel processors and Intel-compatible processors including AMD. Today, IA-32 is often generically called i386, x86-32, and x86. The x86 architecture is the 32-bit architecture used on Intel and Intel-compatible processors, including AMD processors. x64 is today's de facto standard for processors that are built on a 64-bit architecture. Surprisingly, the x64 (also referred to as AMD64 and EM64T, was created by AMD instead of Intel and was later adopted by Intel and other processor manufacturers. It should be noted that x64 is different from Intel Itanium (IA-64 processors), which was Intel's earlier attempt at a mass produced 64-bit processor.

### ExamAlert

Be sure you understand the differences between the 32-bit and 64-bit versions of Windows 7 and when you should use each one if given a scenario.

---

## Cram Quiz

1. Which of the following was not an improvement of Windows 7 over Windows Vista?
  - A. Thicker taskbar
  - B. Gadgets integrated directly into the desktop
  - C. Use of libraries to replace the old documents, pictures, and similar folders
  - D. BitLocker



2. Which edition of Windows 7 is the minimum needed to fully support HomeGroups and DVD Video Playback and authoring?
- A. Windows 7 Home Basic
  - B. Windows 7 Home Premium
  - C. Windows 7 Professional
  - D. Windows 7 Enterprise
3. How much memory does a 32-bit version of Windows support?
- A. 1 GB
  - B. 2 GB
  - C. 4 GB
  - D. 8 GB

## Cram Quiz Answers

1. **D** is correct. BitLocker was introduced with Windows Vista. Answers A, B, and C are incorrect because Windows 7 includes a thicker taskbar, gadgets integrated directly into the desktop, and the use of libraries.
  2. **B** is correct. HomeGroup and DVD Video Playback and authoring are supported by Windows Home Premium, Windows 7 Professional, and Windows 7 Enterprise. However, the minimum you need would be Windows 7 Home Premium. Therefore, the other answers are incorrect.
  3. **C** is correct. The 32-bit version of Windows 7 can only recognize up to 4 GB of memory. It should be noted that not all 32-bit editions of Windows 7 support 4 GB. Therefore, the other answers are incorrect.
-

# Windows 7 Graphical User Interface

- **Supplemental Objectives:** List and describe the main components that make up the graphical user interface used in Windows 7.

## CramSaver

1. The area where the clock and a few select system icons is located on the taskbar is called what?
  - A. Start menu
  - B. The Notification Area
  - C. The Recycle Bin
  - D. The Sidebar
2. What do you call a list that provides a shortcut to a program and is used to provide quick access to recently opened and pinned items from this list?
  - A. Jump List
  - B. Notification list
  - C. Quick Launch
  - D. Window list
3. Which feature in Windows 7 enables you to quickly reveal hidden icons and gadgets?
  - A. Aero Shake
  - B. Aero Peek
  - C. Aero Snap
  - D. Windows Flip 3D

## Answers

1. **B** is correct. The Notification Area is located on the taskbar that has a few system icons that require user attention. Answer A is incorrect because the Start menu is a menu that you open by clicking the Start button to access programs. Answer C is incorrect because the Recycle Bin is used as a temporary area for files that are deleted in Windows. Answer D is incorrect because the Sidebar was a component that held gadgets in Windows Vista but was discontinued in Windows 7.

2. **A** is correct. A Jump List is a list of items you go to frequently. Jump Lists appear on the Start menu next to pinned programs and recently used programs. The Jump Lists can contain recently opened items and items you have pinned to the Jump List. You can also add Jump Lists to the taskbar. Answer B is incorrect because there is no Notification list in the Windows GUI. However, there is a Notification Area located on the taskbar that has a few system icons that require user attention. Answer C is incorrect because the Quick Launch area was used in Windows XP and Windows Vista was replaced with the Jump Lists. Answer D is incorrect because there is no such thing as a Window list.
3. **B** is correct. Aero Peek enables you to peer past all your open windows by making the windows transparent to reveal your hidden icons and gadgets. Answer A is incorrect because Aero Shake enables you to cut through a cluttered desktop so that you can quickly focus on a single window. Answer C is incorrect because Aero Snap is a quick way to resize open windows by dragging them to the edges of your screen. Answer D is incorrect because Windows Flip 3D enables you to flip through all open Windows in a three-dimensional stack without having to click the taskbar.

As with previous versions of Windows, the desktop is the main screen area that you see after you turn on your computer and log on to Windows. Like the top of an actual desk, it serves as a surface for your work. When you open programs or folders, they appear on the desktop. You can also put things on the desktop, such as files and folders, and arrange them however you want, as shown in Figure 1.1.

When you run visible programs or processes in Windows, you run them in a rectangular box called a window. The name *Windows* comes from the ability to run multiple programs or processes at the same time (multitasking) by having multiple Windows open on the desktop.

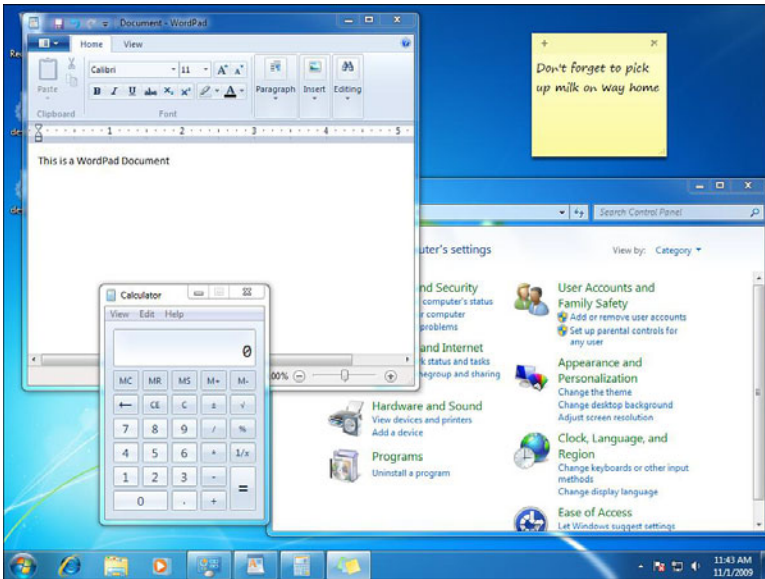


FIGURE 1.1 Windows desktop with taskbar and several running programs.

## Working with the Desktop

To represent the files, folders, and programs, Windows 7 uses icons. A shortcut is an icon that represents a link to an item, rather than the item itself. You can identify shortcuts by the arrow on their icon. Like Windows XP, double-clicking an icon starts or opens the item it represents. If you double-click the Internet Explorer icon, it starts Internet Explorer. If you double-click a report that was written using Microsoft Word, Microsoft Word starts and the report opens. When you double-click a shortcut, the item opens.

By default, when you first start Windows, you see at least one icon on your desktop—the Recycle Bin. Depending on how your computer is configured, after its initial installation, you might have additional desktop icons including the Control Panel, Internet Explorer, or Computer icon. Of course, depending on the user's preference, you can add or remove icons. Some people like to have a clean, uncluttered desktop with few or no icons, and others like to have their frequently used programs, files, and folders available right from the desktop.

To add a shortcut to the desktop, follow these steps:

1. Locate the item (open the Start menu and browse through the installed programs or use Windows Explorer\Computer to find the executable, data file, or folder) that you want to create a shortcut for.
2. Right-click the item, click **Send To**, and then click **Desktop (create shortcut)**. The shortcut icon appears on your desktop.

To add or remove common desktop icons such as Computer, your personal folder, Network, the Recycle Bin, Internet Explorer, and Control Panel, do the following:

1. Right-click an empty area of the desktop and then click **Personalize**.
2. In the left pane, click **Change desktop icons**.
3. Under Desktop icons, select the checkbox for each icon that you want to add to the desktop, or clear the checkbox for each icon that you want to remove from the desktop, and then click **OK**.

To remove an icon from the desktop, right-click the icon, and then click **Delete**. If the icon is a shortcut, only the shortcut is removed; the original item is not deleted.

To move a file from a folder to the desktop, do the following:

1. Open the folder that contains the file.
2. Drag the file to the desktop.

By default, Windows lines up the icons in columns on the left side of the desktop. However, you can move an icon by dragging it to a new place on the desktop.

You can have Windows automatically arrange your icons. Right-click an empty area of the desktop, click **View**, and then click **Auto Arrange**. Windows lines up your icons starting in the upper-left corner, locking them into place. To unlock the icons so that you can move them again, click **Auto Arrange** again, clearing the check mark next to it.

By default, Windows spaces icons evenly on an invisible grid. To place icons closer together or with more precision, turn off the grid. Right-click an empty area of the desktop, click **View**, and then click **Align to Grid** to clear the check mark. Repeat these steps to turn the grid back on.

To move or delete a bunch of icons at once, you must first select all of them. Click an empty area of the desktop and drag the mouse to surround the icons with the rectangle that appears. Then release the mouse button. Now you can drag the icons as a group or delete them.

### Note

In a list of items, you can click on sequential items such as files and folders by clicking the first item, pressing the Shift key, and using the arrows on the keyboard or clicking with the mouse. To select non-sequential items, click and hold down the Ctrl key and use the mouse to select each item.

To temporarily hide all of your desktop icons without actually removing them, right-click an empty part of the desktop, click **View**, and then click **Show Desktop Icons** to clear the checkmark from that option. To get the icons back, click the **Show Desktop Icons** option again.

### Note

The very right edge of the taskbar is a hidden Show Desktop button.

## Windows 7 Taskbar

The taskbar is the long horizontal bar at the bottom of your screen. Unlike the desktop, which can be obscured by open windows, the taskbar is almost always visible. As shown in Figure 1.2, it has three main sections:

- ▶ The Start button opens the Start menu.
- ▶ The middle section shows you which programs and files you have open and enables you to quickly switch between them.
- ▶ The Notification Area includes a clock and icons (small pictures) that communicate the status of certain programs and computer settings.

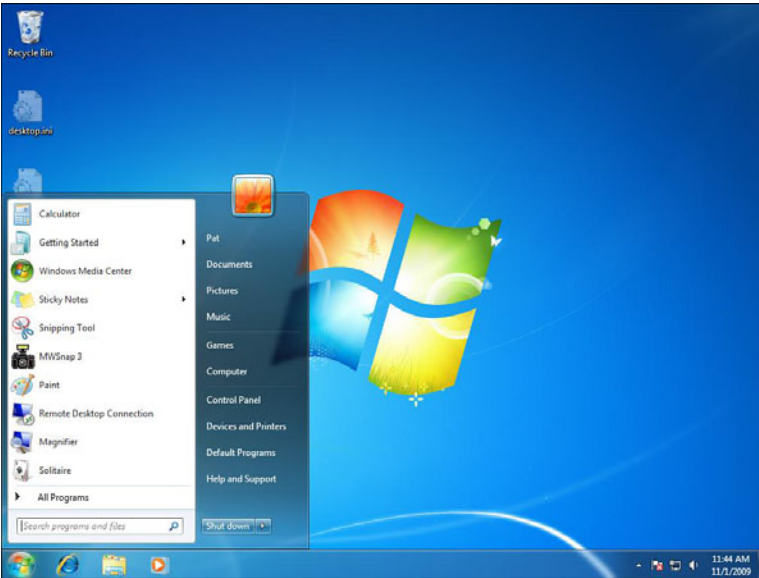


FIGURE 1.2 Windows taskbar with open Start menu.

## Windows 7 Start Menu

To start programs and open folders, you use the Start menu. As the name implies, the Start menu provides a list of choices of items you can launch. It also enables you to search for files, folders, and programs; adjust computer settings; get help with the Windows operating system; turn off the computer; and log off from Windows or switch to a different user account. To open the Start menu, click the Start button in the lower-left corner of your screen or press the Windows logo key on your keyboard.

The Start menu has three basic parts, as illustrated previously in Figure 1.2:

- ▶ The large left pane shows a short list of programs on your computer. Your computer manufacturer can customize this list, so its exact appearance varies. Clicking **All Programs** displays a complete list of programs.
- ▶ At the bottom of the left pane is the search box, which enables you to look for programs and files on your computer by typing in search terms.
- ▶ The right pane provides access to commonly used folders, files, settings, and features. It's also where you go to log off from Windows or turn off your computer.

If you don't see the program you want, click **All Programs** at the bottom of the left pane. The left pane displays a long list of programs in alphabetical order, followed by a list of folders. Clicking one of the program icons starts the program, and the Start menu closes. You also see programs that are used to organize programs.

Under the Accessories folder, you find a set of useful applications, including the following:

- ▶ **Calculator:** You can use Calculator to perform simple calculations such as addition, subtraction, multiplication, and division. Calculator also offers the advanced capabilities of a programming, scientific, statistical calculator and converting common number systems, including converting between decimal, binary, and hexadecimal number systems.
- ▶ **Command Prompt:** An entry point for typing computer commands in the Command Prompt window. By typing commands at the command prompt, you can perform tasks on your computer without using the Windows graphical interface.
- ▶ **Notepad:** A basic text-editing program that you can use to create documents.
- ▶ **Paint:** Used to create drawings on a blank drawing area or in existing pictures. Many of the tools you use in Paint are found in the Ribbon, which is near the top of the Paint window.
- ▶ **Run:** A quick way to open programs, files, folders, and (when you're connected to the Internet) websites. You can also use the search box on the Start menu in place of the **Run** command.
- ▶ **Sticky Notes:** Used to write a to-do list, jot down a phone number, or do anything else that you'd use a pad of paper for. You can use Sticky Notes with a tablet pen or a standard keyboard. To write a note using a tablet pen, simply start writing on the note where you want the ink to appear. To type a note, click where you want the text to appear, and then start typing.
- ▶ **Sync Center:** Enables you to check the results of your recent sync activity if you've set up your computer to sync files with a network server. This enables you to access copies of your network files even when your computer isn't connected to the network. Sync Center can tell you if the files synced successfully or if there are any sync errors or warnings.



- ▶ **Windows Explorer:** A file manager application that provides a graphical user interface for accessing the file systems. It is sometimes referred to as the Windows Shell, or simply “Explorer”; not to be confused with Internet Explorer, which is an Internet browser. If you open Computer, Documents, or the C drive folder, you are using Windows Explorer.
- ▶ **WordPad:** A text-editing program you can use to create and edit documents. Unlike Notepad, WordPad documents can include rich formatting and graphics, and you can link to or embed objects, such as pictures or other documents.
- ▶ **Ease of Access folders:** Several programs and settings that can make the computer easier and more comfortable to use. You can add other assistive technology products to your computer if you need more accessibility features. It includes the Ease of Access Center, Magnifier, Narrator, On-Screen Keyboard, and Windows Speech Recognition.
- ▶ **System Tools folder:** A set of tools used to provide many system functions including Character Map (character/font selection tool), Control Panel, Disk Cleanup, Disk Defragmenter, Internet Explorer (No Add-ons), Resource Monitor, System Restore, Task Scheduler, and Windows Easy Transfer.
- ▶ **Windows PowerShell folder:** A command-line shell and associated scripting language that enables you to execute system commands that might not be executable in a graphical interface.

Under the Maintenance folder, you find

- ▶ **Backup and Restore:** Used to back up and restore Windows.
- ▶ **Create a System Repair Disc:** A system recovery option that can help you repair Windows if a serious error occurs. To use system recovery options, you need a Windows installation disc or access to the recovery options provided by your computer manufacturer. If you don’t have either of those choices, you can create a system repair disc to access system recovery options.
- ▶ **Help and Support:** A built-in help system for Windows. It’s a place to get quick answers to common questions, suggestions for troubleshooting, and instructions for how to do things. You can access it by clicking the Start button and clicking **Help and Support**.
- ▶ **Windows Remote Assistance:** A tool that can be used to give remote access to your machine to assist in fixing or overcoming a problem.

The right pane of the Start menu contains links to parts of Windows that you're likely to use frequently. Here they are, from top to bottom:

- ▶ **Personal folder:** Opens your personal folder, which is named for whoever is currently logged on to Windows. For example, if the current user is Patrick Regan, the folder is named Patrick Regan. This folder, in turn, contains user-specific files, including the Desktop, My Documents, My Music, My Pictures, and My Videos folders.
- ▶ **Documents:** Opens the Documents library, where you can access and open text files, spreadsheets, presentations, and other kinds of documents.
- ▶ **Pictures:** Opens the Pictures library, where you can access and view digital pictures and graphics files.
- ▶ **Music:** Opens the Music library, where you can access and play music and other audio files.
- ▶ **Games:** Opens the Games folder, where you can access all of the games on your computer.
- ▶ **Computer:** Opens a window where you can access disk drives, cameras, printers, scanners, and other hardware connected to your computer.
- ▶ **Control Panel:** Opens Control Panel, where you can customize the appearance and functionality of your computer, install or uninstall programs, set up network connections, and manage user accounts.
- ▶ **Devices and Printers:** Opens a window where you can view information about the printer, mouse, and other devices installed on your computer.
- ▶ **Default Programs:** Opens a window where you can choose which program you want Windows to use for activities such as web browsing.
- ▶ **Help and Support:** Opens Windows Help and Support, where you can browse and search Help topics about using Windows and your computer.

At the bottom of the right pane is the Shut down button. Click the **Shut down** button to turn off your computer. Clicking the arrow next to the Shut down button displays a menu with additional options for switching users, logging off, locking, restarting, or sleep.

## The Notification Area

In Windows 7, the Notification Area of the taskbar has been returned to the user's control. By default, only a select few system icons are shown. When Windows 7 determines that a specific condition requires the user's attention, a new icon appears in the Notification Area. Click the icon to access a menu to address the issue or to open the Action Center for more details.

Users can control the notification experience by dragging icons on or off the taskbar. Better yet, every balloon tip that appears in the system has a little wrench icon that enables you to view the cause of the notification and a direct way to disable it.

A popular change to the Notification Area is about showing more information. The default taskbar now reveals both the time and the date. Only system icons appear by default, and users can customize the area to their liking.

You can customize the icons and notifications that appear in the Notification Area by performing either of the following steps:

- ▶ Click the arrow on the left side of the Notification Area to access its Jump List and then click **Customize**.
- ▶ In Control Panel, click **All Control Panel Items**, and then click **Notification Area Icons** for the resulting window shown in Figure 1.3. Customizing the Notification Area enables you to consolidate notifications and reduce the number of icons that present notification balloons to users.

You can customize the following icons and their behaviors:

- ▶ Action Center
- ▶ Power
- ▶ Network
- ▶ Windows Explorer
- ▶ Windows Activation Client
- ▶ Volume
- ▶ Windows Update Automatic Updates

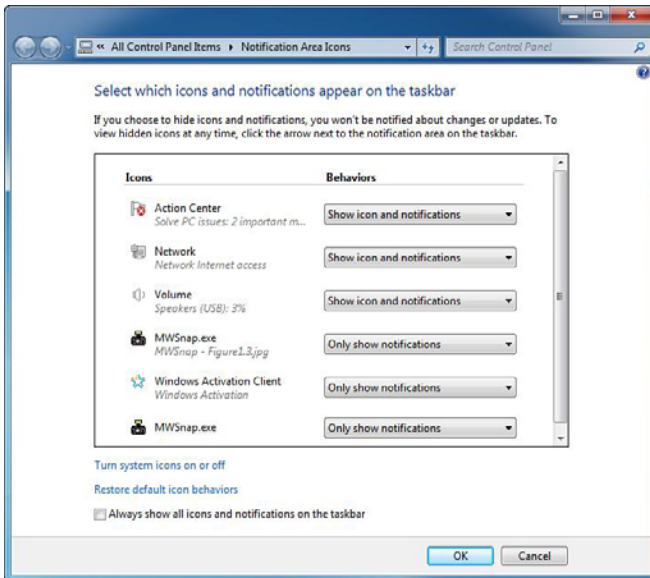


FIGURE 1.3 Customizing the Notification Area.

For each icon, you can set its display behavior to one of the following options:

- ▶ Show icon and notifications
- ▶ Hide icon and notifications
- ▶ Only show notifications

Windows 7 enables you to control the number of system icons displayed in the system tray. In Control Panel, click **All Control Panel Items** and then click **System Icons**. This displays the following list of system icons, each of which has an On/Off option that controls whether the icon appears in the system tray:

- ▶ Clock
- ▶ Volume
- ▶ Network
- ▶ Power
- ▶ Action Center

**Note**

Turning off a system icon not only removes the icon from the system tray, but also turns off displaying any notifications for the icon.

## Customizing the Taskbar and Start Menu

In previous versions of Windows, Windows used a Quick Launch shortcut to quickly start commonly used programs or open commonly used folders or files. Sometimes, an additional icon appeared in the Notification Area to represent running programs, including some programs running in the background. In Windows 7, you can use a single icon for a program on the taskbar, which enables you to start the program and open more program windows. Additionally, Windows 7 helps to provide quick access to recently opened and pinned items from the program's Jump List.

A shortcut enables you to access a program, folder, or document quickly, but a Jump List is a list of items you go to frequently. On the taskbar, Jump Lists appear for programs that you've pinned to the taskbar and programs that are currently running, as shown in Figure 1.4.

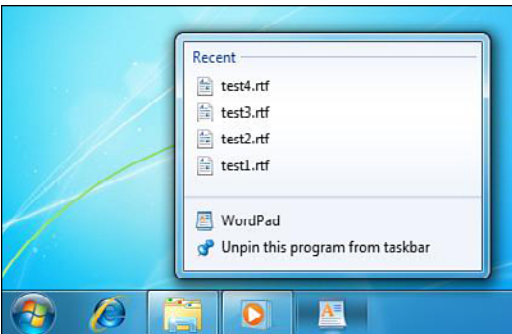


FIGURE 1.4 A Jump List coming from a running program.

For example, if you are working on a large report, which takes you several weeks to write, you can pin the report to your taskbar, work on it day after day, and unpin it when the report is complete. This way, you can quickly access the report each day. If you log off or reboot the computer, the pinned item is still on the taskbar when you log on next time.

To pin something to the taskbar, do one of the following:

- ▶ If the program is already running, right-click the program's icon (or drag the icon toward the desktop) to open the program's Jump List, and then click **Pin to taskbar**.
- ▶ If the program is not running, click **Start**, browse to the program's icon, right-click the icon, and then click **Pin to taskbar**, as shown in Figure 1.5.
- ▶ You can also pin a program's shortcut from the desktop to the taskbar by simply dragging the shortcut to the taskbar. If the shortcut is to a file, then the program used to open it is pinned to the desktop, and the file is pinned to the program's Jump List.

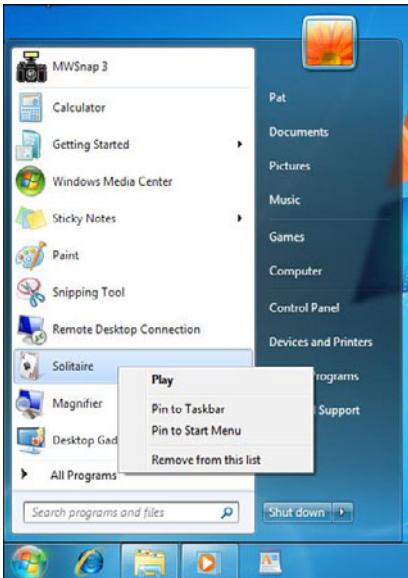


FIGURE 1.5 By right-clicking a program, you can pin to the taskbar or Start menu.

If you right-click the document/program, you can remove it from the taskbar by clicking again to unpin the document or program.

You can also use Jump Lists for the Start menu and programs. You can pin program shortcuts to the top of the Start menu so you can open them quickly and conveniently. There are two methods by which you can pin a program to the Start menu:

- ▶ Click **Start**, browse to the program, right-click the program, and click **Pin to Start menu**. The program's icon will now always appear at the top of the Start menu.

- ▶ Click **Start**, browse to the program, and then drag it to the top left of the Start menu.

**Note**

You can pin a program from the Start menu to the taskbar, but not from the taskbar to the Start menu.

Jump Lists appear on the Start menu next to pinned programs and recently used programs. The Jump Lists can contain recently opened items and items you have pinned to the Jump List.

**Note**

Jump Lists don't appear in All Programs on the Start menu.

In previous Windows versions, icons for the default web browser and email program were pinned to the top of the Start menu. In Windows 7, the pinned area of the Start menu remains, but is empty for a cleaner look. However, you can still pin programs to the top of the Start menu just like in previous Windows versions.

In addition, the Connect to and Network links are removed from the Start menu. Instead, use the Network icon on the taskbar to view available connections or open the Networking and Sharing Center. You can also view computers that are accessible on your network in the navigation pane in any Windows Explorer window.

Perform the following steps to turn window arrangement options on and off:

1. Navigate to Control Panel. Click **Ease of Access Center**. Under Explore all settings, click **Make it easier to focus on tasks**.
2. To turn automatic window arrangement off, scroll toward the bottom of the window, and under Make it easier to manage windows, select the checkbox labeled **Prevent windows from being automatically arranged when moved to the edge of the screen**.
3. To turn automatic window arrangement back on, clear the checkbox labeled **Prevent windows from being automatically arranged when moved to the edge of the screen**.

There are many ways to customize the taskbar to suit your preferences. For example, you can drag the entire taskbar to the left, right, or top edge of the screen. You can make the taskbar larger by dragging the edge of the taskbar.

If you right-click the taskbar and select **Properties**, you can use the Taskbar and Start Menu Properties dialog box, shown in Figure 1.6, to lock the taskbar, auto-hide the taskbar, use small icons, or change the location of the taskbar. You can also customize the Notification Area. If you select the **Start Menu** tab and click the **Customize** button, you can choose which links, icons, or menus appear in the Start menu.

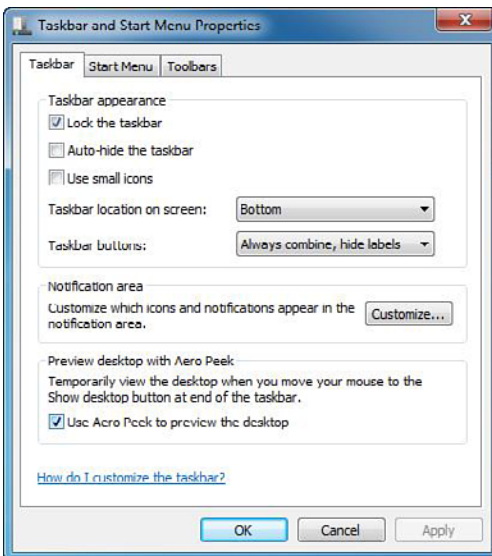


FIGURE 1.6 The Taskbar and Start Menu Properties dialog box.

## Working with Open Windows

Windows 7 automatically resizes the open windows that you drag to the edges of your desktop so you can organize, compare, and read them. This Automatic window arrangement is turned on by default, but you can turn it off and move windows around on the desktop, just as was done with previous Windows versions.

Maximizing a window helps you focus on a single item without the distraction of other open windows.



- ▶ To maximize a window, drag the title bar of a window to the top of the screen.
- ▶ To return the window to its original size, drag the title bar away from the top of the screen.

There are additional ways to maximize an open window, including

- ▶ Double-click the top of an open window just below the top edge. Double-click the top of a maximized window to reduce the window to a smaller size.
- ▶ Shift + right-click a program's icon, or a thumbnail of an open window, and click **Maximize** or **Minimize**. If multiple windows are running for a program, click **Maximize all windows** or **Minimize all windows**.
- ▶ Press the Windows logo key + up arrow to maximize a window. Press the Windows logo key + down arrow to restore the window.

If you minimize a window by pressing the Windows logo key + down arrow, restore it by clicking on its thumbnail on the taskbar or by pressing Shift + right-clicking on the program's icon on the taskbar and then clicking **Restore**.

You can rearrange and organize all program icons on the taskbar (including pinned programs and running programs that are not pinned) so they appear in the order you prefer.

To rearrange the order of program icons on the taskbar, simply drag an icon from its current position to a different position on the taskbar. You can rearrange programs as often as you like. You can also rearrange an icon that appears in the taskbar's Notification Area by dragging the icon to a different position.

All open files from the same program are always grouped together, even if you did not open them one after the other. This is done so that all previews for an open program can be viewed together at the same time.

You can customize how program icons appear and how they group together on the taskbar. You can also change the size of the icons, which changes the height of the taskbar as well. The following options are available for maintaining the icons on the taskbar:

- ▶ Always combine, hide labels. Each program is a single icon without labels, even when multiple items for a program are open. This is the default setting, resulting in a clean and uncluttered taskbar.

- ▶ Combine when taskbar is full. Each open item has an individual, labeled icon.

When the taskbar becomes crowded, programs with multiple open items collapse into a single program icon. Clicking the icon displays a list of the items that are open. Both this and the Never Combine option resemble the look and behavior of earlier Windows versions.

## Gadgets

Windows 7 contains mini-programs called *gadgets*, which offer information at a glance and provide easy access to frequently used tools. Although they were originally introduced in Windows Vista, they differ because gadgets can be placed anywhere within the desktop. In Windows Vista, gadgets had to be placed on the Windows Sidebar, which no longer exists in Windows 7. Some examples of gadgets include displaying a picture slide show, viewing continuously updated headlines, or viewing a clock, as shown in Figure 1.7. If you are running Windows Aero, you can use the Aero Peek feature to temporarily view your desktop gadgets without minimizing or closing the windows you're working with.



FIGURE 1.7 Gadgets (Slide Show, Feed Headlines, and Clock) located on the desktop and an open Desktop Gadget Gallery.

To add a gadget, do the following:

1. Right-click the desktop and click **Gadgets**.
2. Double-click a gadget to add it.

To remove a gadget, right-click the gadget and then click **Close Gadget**.

You can drag a gadget to a new position anywhere on the desktop. You can also install multiple instances of gadget; for example, to see two time zones for the clock or to get different headlines.

To configure a gadget, right-click the gadget and choose the appropriate option. For example, if you right-click the Clock gadget, you can close the Clock, keeping it on top of your open windows, and changing the Clock's options (such as its name, time zone, and appearance).

Before you can add a gadget, it must be installed on your computer. To see which gadgets are installed on your computer, do the following:

1. Right-click the desktop and click **Gadgets**.
2. Click the scroll buttons to see all the gadgets.
3. To see information about a gadget, click the gadget, and then click **Show details**.

You can download additional gadgets online from the following website:

<http://windows.microsoft.com/en-US/windows/downloads/personalize?T1=desktop-gadgets>

## Aero Desktop Experience

Windows Aero, introduced with Windows Vista, is the premium visual experience of Windows. It features a transparent glass design with subtle window animations and new window colors. Part of the Windows Aero experience is Windows Flip 3D (shown in Figure 1.8), which is a way to arrange your open windows in a three-dimensional stack that you can quickly flip through without having to click the taskbar. The keyboard shortcuts for Windows Flip 3D are the Windows key + Tab.

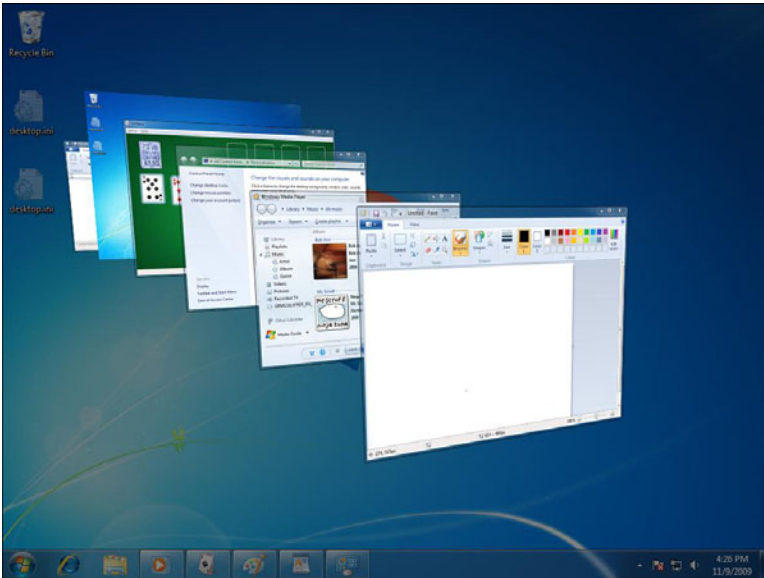


FIGURE 1.8 Windows Flip 3D

Aero also includes taskbar previews for your open windows. When you point to a taskbar button, you see a thumbnail-sized preview of the window, whether the content of the window is a document, a photo, or even a running video. Beyond the new graphics and visual polish, the Windows Aero desktop experience includes smoother window handling, increased graphics stability, and glitch-free visuals, all of which give you a simple, comfortable, and high-quality experience.

Windows 7 includes some new features to work with your desktop applications:

- ▶ **Aero Shake:** If you need to cut through a cluttered desktop and quickly focus on a single window, just click a pane and shake your mouse back and forth. Every open window except that one instantly disappears. Jiggle again—and your windows are back. Note that some windows, such as open dialog boxes, cannot be minimized in this way.
- ▶ **Aero Peek:** Enables you to peer past all your open windows by making all the windows transparent to reveal all your hidden icons and gadgets.
- ▶ **Aero Snap:** A quick way to resize open windows simply by dragging them to the edges of your screen. Depending on where you drag a window, you can make it expand vertically, take up the entire screen, or appear side-by-side with another window.

The following editions of Windows 7 include Aero:

- ▶ Windows 7 Home Premium
- ▶ Windows 7 Professional
- ▶ Windows 7 Enterprise
- ▶ Windows 7 Ultimate

Aero is not included in Windows 7 Home Basic or Windows 7 Starter.

### ExamAlert

Be sure you know what editions of Windows 7 support Windows Aero.

---

## Cram Quiz

1. What do you call the long horizontal bar at the bottom of the screen that includes the running programs, the Start button, and the Notification Area?
  - A. Desktop
  - B. Taskbar
  - C. Windows Explorer
  - D. Alert Center
  
2. What replaced the Quick Launch shortcut?
  - A. Notification Area
  - B. Alert Center
  - C. Recycle Bin
  - D. Jump Lists
  
3. Which features are new to Windows 7? (Choose all that apply.)
  - A. Aero Shake
  - B. Aero Peek
  - C. Aero Snap
  - D. Windows Flip 3D

## Cram Quiz Answers

- 1. B** is correct. The taskbar is the long horizontal bar at the bottom of the screen. Answer A is incorrect because the desktop is the main screen area that you use after you turn on your computer and log on to Windows. Answer C is incorrect because the Windows Explorer is the program that enables you to manage files and folders. Answer D is incorrect because the Alert Center is a program that notifies you of security and maintenance problems.
  - 2. D** is correct. A Jump List appears for programs that you've pinned to the taskbar and for programs that you are currently running. It helps you quickly access a program, folder, or document quickly. Answer A is incorrect because the Notification Area contains system icons that are alerting you of their status. Answer B is incorrect because the Alert Center notifies you of maintenance and security alerts. Answer C is incorrect because the Recycle Bin is used as a temporary storage area for files and folders that you delete.
  - 3. A, B, and C** are correct. If you need to cut through a cluttered desktop and quickly focus on a single window, just click a pane and shake your mouse back and forth (Aero Shake). Every open window except the one instantly disappears. Aero Peek enables you to peer past all of your open windows by making all of the Windows transparent. Aero Snap is a quick way to resize open windows. Answer D is incorrect because Windows Flip 3D was introduced in Windows Vista and enables you to arrange your windows in a three-dimensional stack that you can quickly flip through without having to click the taskbar.
-

# Review Questions

1. Which operating system was the most popular operating system when Windows 7 was released?
  - A. Windows XP
  - B. Windows Vista
  - C. Windows 2003 Workstation
  - D. Windows 98
2. Which version of the kernel does Windows 7 use?
  - A. 5
  - B. 5.1
  - C. 6
  - D. 7
3. What is the maximum number of applications you can run concurrently with the Windows 7 Starter?
  - A. 1
  - B. 2
  - C. 3
  - D. Limited only by the hardware
4. Which editions of Windows 7 include all features that Windows 7 has to offer? (Choose two answers.)
  - A. Windows 7 Home Premium
  - B. Windows 7 Professional
  - C. Windows 7 Enterprise
  - D. Windows 7 Ultimate
5. Which of the following support added Windows 7 to a Windows domain? (Choose all that apply.)
  - A. Windows 7 Starter
  - B. Windows 7 Home Basic
  - C. Windows 7 Home Premium
  - D. Windows 7 Professional
  - E. Windows 7 Enterprise
  - F. Windows 7 Ultimate

6. What is the disadvantage of using a 64-bit version of Windows 7 when running applications?
- A. You are not able to run legacy 16-bit applications directly on Windows 7.
  - B. You are only able to run up to three legacy 16-bit applications.
  - C. You need to have 16-bit drivers available to use 16-bit applications.
  - D. Your 16-bit applications run slowly.
7. What do you call the main screen area that you see after you turn on your computer and log on to Windows?
- A. Desktop
  - B. Taskbar
  - C. Windows Explorer
  - D. Notification Area
8. Where do you place your gadgets?
- A. Notification Area
  - B. Start menu
  - C. Desktop
  - D. Taskbar
9. What do you call the feature that enables you to shake away the cluttered desktop to quickly focus on a single window?
- A. Aero Shake
  - B. Aero Peek
  - C. Aero Snap
  - D. Windows Flip 3D
10. Which of the following include Windows Aero? (Choose all that apply.)
- A. Windows 7 Home Premium
  - B. Windows 7 Home Basic
  - C. Windows 7 Professional
  - D. Windows 7 Ultimate



## Review Question Answers

- 1. A** is correct. Although Windows XP was released in 2001, it was still the most popular operating system when Windows 7 was released. Answer B is incorrect because Windows Vista was heavily criticized and never became as popular as Windows XP. Answer C is incorrect because Windows 2003 Workstation does not exist. Answer D is incorrect because although Windows 98 was popular long ago, Windows XP became more popular, and it replaced Windows 98.
- 2. D** is correct. Windows 7 uses the 7.0 version of the kernel. Answer A is incorrect because Windows 2000 used the 5.0 kernel. Answer B is incorrect because Windows XP uses the 5.1 kernel. Answer C is incorrect because Windows Vista uses 6.0 kernel.
- 3. D** is correct. Windows 7 Starter is an edition targeted specifically for small form factor PCs. It is only available for 32-bit platforms. Initially, Windows 7 Starter edition could only support up to three concurrent programs. Since then, Microsoft has eased this restriction and now enables you to run as many programs as you desire, being limited only by your hardware such as the amount of RAM. Therefore, Answers A, B, and C are incorrect.
- 4. C and D** are correct. Windows 7 Enterprise is targeted at large Enterprise customers. Windows 7 Ultimate is targeted for technical enthusiasts who want all Windows 7 features. Windows 7 Enterprise edition requires a volume license, but Microsoft Windows 7 Ultimate does not. Answers A and B are not correct because Windows 7 Home Premium and Windows 7 Professional do not include the language packs and do not have some of the more advanced enterprise applications, such as BitLocker, BitLocker To Go, AppLocker, DirectAccess, and BranchCache.
- 5. D, E, and F** are correct. The only versions that support adding to a domain are Windows 7 Professional, Enterprise, and Ultimate. Windows 7 Starter, Home Basic, and Home Premium do not support adding to a domain. Therefore, answers A, B, and C are incorrect.
- 6. A** is correct. Although 64-bit versions of Windows 7 can address more memory and can process more at one time, they cannot directly support legacy 16-bit applications. Therefore, the other answers are incorrect. If you have a 16-bit application and you want to run the application on a 64-bit version of Windows 7, you should try using XP Mode.
- 7. A** is correct. The desktop is the main screen area that you see after you turn on your computer and log on to Windows. You can think of it as similar to a desk, which serves as a surface for your work. Answer B is incorrect because the taskbar is a long horizontal bar at the bottom of the screen. Answer C is incorrect because the Windows Explorer is the program that enables you to manage files and folders. Answer D is incorrect because the Notification Area is the area on the taskbar that holds system icons to let you know of an event.
- 8. C** is correct. Unlike in Windows Vista, Gadgets in Windows 7 can be placed anywhere on the desktop. They cannot be placed on the Start menu, taskbar, or Notification Area; therefore, Answers A, B, and D are incorrect.

9. **A** is correct. If you need to cut through a cluttered desktop and quickly focus on a single window, just click a pane and shake your mouse back and forth. Every open window except the one selected disappears. Answer B is incorrect because Aero Peek enables you to peer past all your open windows by making all the windows transparent. Answer C is incorrect because Aero Snap is a quick way to resize open windows. Answer D is incorrect because Windows Flip 3D enables you to arrange your windows in a three-dimensional stack that you can quickly flip through without having to click the taskbar.
10. **A**, **C**, and **D** are correct. Windows Aero can be found on Windows 7 Home Premium, Windows 7 Professional, Windows 7 Enterprise, and Windows 7 Ultimate. It is not included in Windows 7 Home Basic or Windows 7 Starter. Therefore, Answer B is incorrect.

*This page intentionally left blank*

## CHAPTER 2

# Installing, Upgrading, and Migrating to Windows 7

### **This chapter covers the following 70-680 Objectives:**

- ▶ Installing, Upgrading, and Migrating to Windows 7:
  - ▶ Perform a clean installation
  - ▶ Upgrade to Windows 7 from previous versions of Windows
  - ▶ Migrate user profiles
- ▶ Deploying Windows 7:
  - ▶ Capture a system image
  - ▶ Prepare a system image for deployment
  - ▶ Deploy a system image
  - ▶ Configure a VHD
- ▶ Monitoring and Maintaining Systems That Run Windows 7:
  - ▶ Configure updates to Windows 7

This chapter discusses how to install and deploy Windows 7 so that you can start using it. If you have a new machine, you do a clean installation. If you have an older machine with an operating system already on it, you need to choose between doing a clean installation or upgrading the current installation. Either way, you need to make sure you have the system resources available that allow for some modest growth.

# Installing Windows 7

- ▶ **Installing, Upgrading, and Migrating to Windows 7**
  - ▶ **Perform a clean installation**
  - ▶ **Upgrade to Windows 7 from previous versions of Windows**
- ▶ **Monitoring and Maintaining Systems That Run Windows 7**
  - ▶ **Configure updates to Windows 7**

## CramSaver

1. What is the minimum amount of RAM and processor required for the 64-bit Windows 7 Professional Edition?
  - A.** 512 MB and 1 GHz processor
  - B.** 1 GB and 1 GHz processor.
  - C.** 2 GB and 800 MHz
  - D.** 2 GB and 1 GHz
  - E.** 1 GB and 1.2 GHz
  
2. If you have Windows XP Professional installed, what would it take to upgrade to Windows 7 Professional?
  - A.** You need to first upgrade to Windows Vista Business and then upgrade to Windows 7 Professional.
  - B.** You need to install Windows XP SP3 before upgrading to Windows 7 Professional.
  - C.** You need to migrate the user settings using the Windows Easy Transfer and then perform a clean install of Windows 7.
  - D.** You need to migrate the user settings using the Windows Easy Transfer and then perform an upgrade to Windows 7.

## Answers

1. **D** is correct. For the 64-bit Windows 7 Professional Edition, you need a 1-GHz processor and 2 GB of RAM. Therefore, the other answers are incorrect.
2. **A** is correct. There is not a direct upgrade from Windows XP to Windows 7. Therefore, you need to upgrade to Windows Vista Business first and then upgrade to Windows 7. Of course, this is not recommended and can be very costly if you have to purchase Windows Vista and Windows 7.

Before installing or upgrading to Windows 7, you need to look at the system and verify whether it has the necessary hardware to effectively run Windows 7. Table 2.1 outlines the hardware requirements for installing Windows 7.

TABLE 2.1 **Minimum Hardware Requirements for Installing Windows 7**

Hardware	Starter	Home Basic	Other Versions of Windows 7
Processor	800 MHz	1 GHz	1 GHz
RAM	512 MB	1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)	1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
GPU	SVGA	DirectX 9	Aero Capable GPU that supports DirectX 9 with a WDDM driver, Pixel Shader 2.0 and 32 bits per pixel
Video RAM	Not applicable	Not applicable	128 MB
HDD	20 GB	40 GB	40 GB
Free HDD Space	16 GB available hard disk space (32-bit)	16 GB available hard disk space (32-bit) or 20 GB (64-bit)	16 GB available hard disk space (32-bit) or 20 GB (64-bit)
Optical Drive	CD	DVD	DVD

#### Note

Windows XP Mode requires an additional 1 GB of RAM and an additional 15 GB of available hard disk space.

Of course, like older versions of Windows, if a system has a faster processor or additional RAM, your system runs faster, and it is almost always recommended. In addition, as you patch Windows, the C:\Windows\Winsxs folder can take significant disk space as it holds copies of dynamic linked libraries (DLLs) and other components, all of which are used to make your system more reliable.

Although 32-bit versions of Windows 7 can support up to 4 GB of RAM, the 64-bit versions of Windows 7 can support up to 192 GB. Table 2.2 outlines the maximum memory recognized by Windows 7. In addition, although all editions of Windows 7 can support multiple core CPUs, only Windows 7 Professional, Ultimate, and Enterprise can support dual processors.

**ExamAlert**

You need to know the minimum memory requirements and the maximum memory recognized by Windows 7.

TABLE 2.2 **Maximum Memory Recognized by Windows 7**

Version	Limit in 32-Bit Windows	Limit in 64-Bit Windows
Windows 7 Ultimate	4 GB	192 GB
Windows 7 Enterprise	4 GB	192 GB
Windows 7 Professional	4 GB	192 GB
Windows 7 Home Premium	4 GB	16 GB
Windows 7 Home Basic	4 GB	8 GB
Windows 7 Starter	2 GB	2 GB

## Windows 7 Installation Methods

To start the installation process, you insert the Windows 7 Installation DVD into the drive and boot from the DVD drive. If the system does not boot from the DVD disc, you might need to modify the boot order specified in the BIOS setup program. You can also boot and install from a USB device. All packaged retail editions of Windows 7 (except for Home Basic) include both 32- and 64-bit software.

Similar to Windows Vista, the process to install Windows 7 is pretty straightforward. During the installation, you can choose one of three installation methods:

- ▶ **Installing a custom version of Windows:** With this method, you perform a clean installation, including installing Windows on a new system with no previous operating system or completely replace your current operating system. You can also use this option to specify which drive or partition on which to install Windows 7 and if you need to establish a multiboot system.
- ▶ **Upgrading to Windows 7:** Used to keep your files, settings, and programs from your current version of Windows (also known as an in-place upgrade). If your version of Windows can't be upgraded, you need to choose Custom.
- ▶ **Reinstalling Windows 7:** Choose this method if you want to restore default Windows settings or if you are having trouble with Windows and need to reinstall it by performing a custom installation.

## Windows Clean Installation

There are several methods to perform a clean installation of Windows 7.

- ▶ **Running Windows 7 installation from CD/DVD or USB boot device:** Installing from the product CD/DVD is the simplest way to install Windows 7.
- ▶ **Running Windows 7 installation from a Network Share:** Instead of a CD/DVD, the Windows 7 installation files can be stored in a network share. Generally, the network source is a shared folder on a file server. If your computer does not currently have an operating system, start the computer by using Windows Preinstallation Environment (PE). If your computer already has an operating system, you can start the computer with the old operating system.

### Note

Windows PE is a minimal 32- or 64-bit operating system with limited services, built on the Windows 7 kernel. Windows PE is used to install and repair a Windows operating system, which is particularly useful if your system does not boot. It can also be used to install Windows on systems over the network that do not support Preboot eXecution Environment (PXE) boot.

- ▶ **Installing Windows 7 by Using an Image:** With this method, you install Windows 7 to a reference computer and prepare the reference computer for duplication. You capture the volume image to a Windows Imaging (WIM) file by using the ImageX tool and then use the deployment tools, such as ImageX, Windows Deployment Services (WDS), or Microsoft Deployment Toolkit (MDT) to deploy the captured image.

## Upgrading Windows

You must perform an in-place upgrade when you do not want to reinstall all of your applications. In addition, you can consider performing an upgrade when:

- ▶ You do not have storage space to store your user state.
- ▶ You are not replacing existing computer hardware.
- ▶ You plan to deploy Windows on only a few computers.



Although you can upgrade computers in large enterprises, it is usually recommended that you perform a clean installation by using images followed by migrating user settings and data.

You can upgrade from a similar version of Windows Vista to Windows 7. In all other instances, you have to perform a custom install to replace your previous Windows. For example, you can upgrade Windows Vista Ultimate 32-bit to Windows 7 Ultimate 32-bit or a Windows Vista Business 64-bit to Windows 7 Professional 64-bit. You also need to perform a custom install from Windows XP to Windows 7. Table 2.3 outlines which versions and editions of Windows can be upgraded and which require a custom installation.

TABLE 2.3 **Upgrading to Windows 7**

		Windows 7 Home Premium		Windows 7 Professional		Windows 7 Ultimate	
		32-bit	64-bit	32-bit	64-bit	32-bit	64-bit
<b>Windows XP</b>	<b>32-bit</b>	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
	<b>64-bit</b>	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
<b>Windows Vista Starter</b>	<b>32-bit</b>	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
	<b>64-bit</b>	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install
<b>Windows Vista Home Basic</b>	<b>32-bit</b>	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	<b>64-bit</b>	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
<b>Windows Vista Home Premium</b>	<b>32-bit</b>	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	<b>64-bit</b>	Custom Install	In-Place Upgrade	Custom Install	Custom Install	Custom Install	In-Place Upgrade
<b>Windows Vista Business</b>	<b>32-bit</b>	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade	Custom Install
	<b>64-bit</b>	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install	In-Place Upgrade

TABLE 2.3 Continued

		Windows 7 Home Premium		Windows 7 Professional		Windows 7 Ultimate	
		32-bit	64-bit	32-bit	64-bit	32-bit	64-bit
<b>Windows Vista Ultimate</b>	<b>32-bit</b>	Custom Install	Custom Install	Custom Install	Custom Install	In-Place Upgrade	Custom Install
	<b>64-bit</b>	Custom Install	Custom Install	Custom Install	Custom Install	Custom Install	In-Place Upgrade

**ExamAlert**

One of the criticisms of Windows 7 is that there is no direct upgrade from Windows XP to Windows 7. If you need to upgrade a system, you need to upgrade Windows XP to Windows Vista and then upgrade Windows Vista to Windows 7.

An in-place upgrade does not support cross architecture. This means that you cannot upgrade from 32-bit to 64-bit or vice versa. An in-place upgrade does not support cross language. In both cases, you need to perform a clean installation and the necessary migration.

When you install/upgrade Windows 7, you should follow these guidelines:

- ▶ Update your antivirus program, run it, and then disable it. After you install Windows, remember to re-enable the antivirus program, or install new antivirus software that works with Windows 7.
- ▶ Back up your files. You can back up files to an external hard disk, a DVD or CD, or a network folder.
- ▶ Connect to the Internet. Make sure your Internet connection is working so that you can get the latest installation updates. These updates include security updates and hardware driver updates that can help with installation. If you don't have an Internet connection, you can still upgrade or install Windows.

You can perform an upgrade between two editions of Windows 7 by using Windows Anytime Upgrade. Different from Windows Vista, Windows 7 Anytime Upgrade does not require any discs because no matter which edition is installed, the entire operating system is placed on the computer's local drive.

Upgrading your computer to your new edition of Windows 7 can take between 10 and 90 minutes. You do not have access to your programs and files during this time.

### Note

Windows Enterprise is excluded from Windows Anytime Upgrade because it is only available through volume license and it includes all features available for Windows 7.

The steps to perform an upgrade include the following:

1. Insert the Windows 7 DVD.
2. Click **Install now** on the Install Windows screen.
3. Click the **Install Now** button and the computer begins the installation.
4. After some files are copied, choose the **Install** option.
5. When it asks to get important updates for installation, click the **Go online to get the latest updates for installation** option.
6. When it asks you to accept the license terms, click the appropriate checkbox and then click the **Next** button.
7. Toward the end of the installation process, specify a Windows login name and password.
8. Set the time and date.

For more information upgrading to Windows 7, visit the following websites:

<http://windows.microsoft.com/en-us/windows7/help/upgrading-from-windows-vista-to-windows-7>

[http://technet.microsoft.com/en-us/library/ee461274\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee461274(WS.10).aspx)

## Windows 7 Upgrade Advisor

In general, if your PC can run Windows Vista, it can run Windows 7. But if you're not running Windows Vista, or are just not sure if your system is ready to run Windows 7, you can use the Windows 7 Upgrade Advisor. The Windows 7 Upgrade Advisor can be found here:

<http://www.microsoft.com/windows/windows-7/get/upgrade-advisor.aspx>

The only prerequisite to run the Windows 7 Upgrade Advisor is to have .NET 2.0 Framework or higher and MSXML 6.0. After you've downloaded, installed, and run the Windows 7 Upgrade Advisor, the program displays a report telling you if your PC can run Windows 7 and if there are any known compatibility issues. If an issue can be resolved, you get suggestions for next steps.

## Troubleshooting an Upgrade or Migration to Windows 7

If you experience problems during an upgrade or migration to Windows 7, you use standard troubleshooting methodology to isolate the problem. Of course, to gather information, you should

- ▶ **Review and research error messages:** When an error message is displayed, use your favorite search engine to research the meaning of the message and how to overcome the problem with the proper solution.
- ▶ **Check logs:** During setup, Windows 7 produces log files (located in `Windows\panther`) into which it records setup progress and information relating to problems encountered during setup.
- ▶ **Verify system meets minimum requirements:** A common reason for an upgrade to fail is that the computer does not meet the minimum hardware requirements to support the edition of Windows 7 that you are installing.
- ▶ **Check devices and BIOS:** If Windows setup encounters a compatibility problem with a device or with the computer's BIOS, the upgrade might fail.
- ▶ **Verify installation media:** Make sure that the installation media is not damaged or corrupt.

# Windows Updates

After installing Windows, check to see if Microsoft has any fixes, patches, service packs, and device drivers and apply them to the Windows system. By adding fixes and patches, you keep Windows stable and secure. If there are many fixes or patches, Microsoft releases them together as a service pack. To update Windows 7, Internet Explorer, and other programs that ship with Windows, go to Windows Update in the Control Panel or click the **Start** button, select **All Programs**, and select **Windows Update**. Windows then scans your system to see what you have installed and gives you a list of suggested components. This system check assures that you get the most up-to-date and accurate versions of anything you choose to download from the site.

To help users with the Windows updates, Windows 7 also offers Dynamic Update and Auto Update. Dynamic Update is a feature built into Windows Setup that automatically checks for new drivers, compatibility updates, and security fixes while Windows is being installed. All that is required is that you have a working connection to the Internet. During installation, you can choose to have Dynamic Update check for updates. Dynamic Update automatically downloads any device or application updates and uses these replacement files instead of the installation files, thereby ensuring you have the latest updates available. By updating your installation files as needed, Windows can quickly integrate new, certified device drivers, critical security fixes, and compatibility updates.

Microsoft routinely releases security updates on the second Tuesday of each month on what is known as “Patch Tuesday.” Most other updates are released as needed. After you install Windows, you can use Auto Update to ensure that critical security and compatibility updates are made available for installation automatically, without significantly affecting your regular use of the Internet. Auto Update works in the background when you are connected to the Internet to identify when new updates are available and to download them to your computer. The download is managed so that it does not affect the performance during web surfing, and it picks up where it left off if the download is interrupted.

When the download is completed, you are notified and prompted to install the update. You can install it then, get more details about what is included in the update, or let Windows remind you about it later. Some installations might require you to reboot, but some do not.

To manually install updates, it is recommended that you click the **Start** button, click **All Programs**, and click **Windows Update**. Then in the left pane, click **Check for updates**, as shown in Figure 2.1.

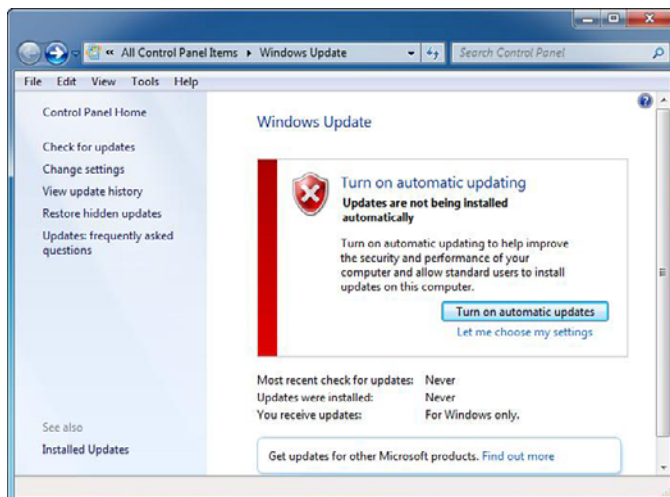


FIGURE 2.1 Windows Update.

To change the Windows Update settings, click the **Change settings** option in the left pane to display the window shown in Figure 2.2. The options enable you to specify whether to download and let you specify which ones to install, specify which updates to install and then download, or just disable Windows Updates all together. You can also specify if Windows Update should check for other Microsoft products other than the operating system and also install software that Microsoft recommends.

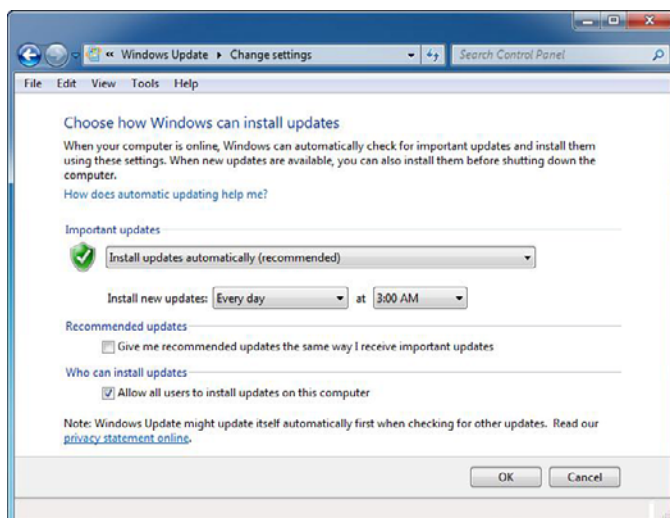


FIGURE 2.2 Choose how Windows can install Updates.

If Windows Update fails to get updates, you should check your proxy settings in Internet Explorer to see if it can get through your proxy server (if any) or firewall. You should also check to see if you can access the Internet, such as accessing the [www.microsoft.com](http://www.microsoft.com) website.

To see all updates that have been installed, click the **View Update History** link in the left pane (shown in Figure 2.1). If you suspect a problem with a specific update, you can then click **Installed Updates** at the bottom of the screen, which opens the Control Panel's Programs. From there, you then see all installed programs and installed updates. If the option is available, you can then remove the update.

## Activating Windows 7

While volume license might not require activation, retail versions of Windows 7 need to be activated after installation. In the Welcome Center, the **Activation Status** entry specifies whether you have activated the operating system. If Windows 7 has not been activated, you can activate the operating system by clicking **More Details** to access the System console and then selecting **Click Here To Activate Windows Now** under Windows Activation.

Unlike in Windows XP, you can easily change the product key used by the operating system except in Original Equipment Manufacturer (OEM) copies of Windows 7. In the System console, click **Change Product Key** under Windows Activation. In the Windows Activation window, type the product key and then click **Next**. As in Setup, you do not need to type the dashes in the product key.

## Restore a Computer to a Previous Windows Installation

When you perform a clean installation of Windows 7 on a hard disk partition that contains an existing Windows installation (assuming you did not reformat the hard disk), the previous operating system, user data, and program files are saved to a `Windows.OLD` folder. If the `Windows.OLD` folder exists on this drive, files from the previous Windows installation are saved during the Windows 7 installation process. Therefore, you can restore the computer to the previous Windows installation by following the directions from the following Microsoft website:

<http://support.microsoft.com/kb/971760>

**ExamAlert**

If you perform an upgrade from an older version of Windows, the old Windows version is placed in the Windows.OLD folder so that you can retrieve old data and restore a computer to the previous Windows version.

## Using BCDEdit

During the boot process, the system ROM BIOS accesses the primary hard drive and reads the master boot record (MBR), which is the first 512 bytes of the hard drive. It contains the disk's primary partition table and a boot loader. A boot loader is a file that contains necessary information that instructs the system how to boot/start an operating system. For Windows Vista and Windows 7, the boot loader starts the Boot Manager (bootmgr), which then reads the partition table to identify the active partition, accesses the Boot Configuration Data (BCD) store, and starts the Windows Boot Manager (winload.exe), which loads Windows.

The active partition or volume that contains the Boot Manager is known as the *system partition/volume*. The partition or volume that contains the Windows operating system files (usually the Windows folder) is called the *boot partition*. It is common for computer systems to have one drive and one partition/volume, which makes the partition both the system partition and the boot partition.

Boot Configuration Data (BCD) is a database store (located in the \Boot\bcd folder on the system volume) that contains the boot-time configuration data used by Microsoft's Windows Boot Manager found with Windows Vista, Windows 7, and Windows Server 2008. To edit the Boot Configuration, you typically use the bcdedit.exe command-line tool.

**Note**

To run the `bcdedit` command, you need to run the command from an elevated command prompt.

**ExamAlert**

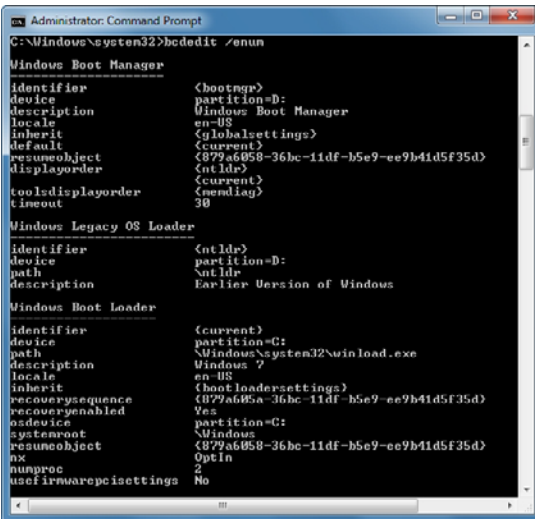
To modify the boot configuration for Windows Vista and Windows 7 systems, you need to use the `bcdedit` command to edit the hidden file that stores the boot configuration.



Before you start making changes using the `bcdedit` command, you need to look at your configuration and record the identifiers. To list the entries in the store, you would execute the following command:

```
bcdedit /enum
```

As you can see in Figure 2.3, the `bcdedit` command identifies the Windows Boot Manager is located on the D drive and the Windows Boot Loader is located on the `C:\Windows\System32\winload.exe`.



```

Administrator: Command Prompt
C:\Windows\system32>bcdedit /enum
Windows Boot Manager
-----
identifier          <bootmgr>
device              partition=D:
description         Windows Boot Manager
locale              en-US
inherit              <globalsettings>
default             <current>
resumeobject        {879a6058-36bc-11df-b5e9-ee9b41d5f35d}
displayorder        <ntldr>
tooldisplayorder    <current>
lineout             <msdiag>
lineout             30
Windows Legacy OS Loader
-----
identifier          <ntldr>
device              partition=D:
path                <ntldr>
description         Earlier Version of Windows
Windows Boot Loader
-----
identifier          <current>
device              partition=C:
path                %SystemRoot%\System32\winload.exe
description         Windows 7
locale              en-US
inherit              <bootloadersettings>
recoverysequence    {879a6058-36bc-11df-b5e9-ee9b41d5f35d}
recoveryenabled     Yes
osdevice            partition=C:
systemroot          %SystemRoot%
resumeobject        {879a6058-36bc-11df-b5e9-ee9b41d5f35d}
nx                  OptIn
numproc             2
usefirmwarepcsettings No
  
```

FIGURE 2.3 Executing the `bcdedit /enum` command.

Every drive or partition on the system is identified as one of the following:

- ▶ **{legacy}**: Describes a drive or partition on which a pre-Windows Vista operating system exists
- ▶ **{default}**: Describes the drive or partition containing the current default operating system
- ▶ **{current}**: Describes the current drive or partition one is booted to

Each drive or partition also includes a global unique identifier (GUID). To display the GUIDs, execute the following command:

```
bcdedit /v
```

Figure 2.4 demonstrates executing the `bcdedit /v` command.

```

Administrator: Command Prompt
C:\Windows\system32\bcdedit /v

Windows Boot Manager
-----
identifier             {9da862c-5cdd-4e70-acc1-f32b344d4795}
device                 partition=D:
description            Windows Boot Manager
locale                 en-US
inherit                {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
default                {879a6059-36bc-11df-b5e9-ee9b41d5f35d}
resumeobject           {879a6058-36bc-11df-b5e9-ee9b41d5f35d}
displayorder           {466f5a88-8af2-4f76-9038-095b170dc21c}
toolsdisplayorder     {879a6059-36bc-11df-b5e9-ee9b41d5f35d}
tooldisplayorder      {c2721d73-1db4-4c62-bf78-c548a880142d}
timeout                30

Windows Legacy OS Loader
-----
identifier             {466f5a88-8af2-4f76-9038-095b170dc21c}
device                 partition=D:
path                  \ntldr
description            Earlier Version of Windows

Windows Boot Loader
-----
identifier             {879a6059-36bc-11df-b5e9-ee9b41d5f35d}
device                 partition=C:
path                  \Windows\system32\winload.exe
description            Windows ?
locale                 en-US
inherit                {6efb52bf-1766-41db-a6b3-0ec5eff72bd7}
recoverysequence       {879a605a-36bc-11df-b5e9-ee9b41d5f35d}
recoveryenabled        Yes
osdevice               partition=C:
systemroot             \Windows
resumeobject           {879a6058-36bc-11df-b5e9-ee9b41d5f35d}
nx                     OptIn
numproc                2
usefirmwarepcsettings No
  
```

FIGURE 2.4 Executing the `bcdedit /v` command.

In addition, you can add the following parameters to the `bcdedit /enum` command to change the information that is displayed:

- ▶ **Active:** Displays all entries in the boot manager display order (default)
- ▶ **Firmware:** Displays all firmware applications
- ▶ **Bootapp:** Displays all boot environment applications
- ▶ **Bootmgr:** Displays the boot manager
- ▶ **Osloader:** Displays all operating system entries
- ▶ **Resume:** Displays all resume from hibernation entries
- ▶ **Inherit:** Displays all inherit entries
- ▶ **All:** Displays all entries

Because the BCD store is essential for your system to boot properly, it is recommended that you back up the BCD settings before you make any changes. To make a backup of your current BCD registry settings, execute the following command:

```
bcdedit /export name_of_file.bcd
```

To restore your BCD registry settings, execute the following command:

```
bcdedit /import name_of_file.bcd
```

To view the `bcdedit` command options, execute the following command:

```
bcdedit /?
```

These options include the following:

- ▶ **/createstore:** Creates a new empty BCD store
- ▶ **/export:** Exports the contents of the system BCD store to a specified file
- ▶ **/import:** Restores the state of the system BCD store from a specified file
- ▶ **/copy:** Makes copies of boot entries
- ▶ **/create:** Creates new boot entries
- ▶ **/delete:** Deletes boot entries
- ▶ **/deletevalue:** Deletes elements from a boot entry
- ▶ **/set:** Creates or modifies a boot entry's elements
- ▶ **/bootsequence:** Specifies a one-time boot sequence
- ▶ **/default:** Specifies the default boot entry
- ▶ **/displayorder:** Specifies the order in which Boot Manager displays its menu
- ▶ **/timeout:** Specifies the Boot Manager Timeout value
- ▶ **/toolsdisplayorder:** Specifies the order in which Boot Manager displays the tools menu
- ▶ **/bootems:** Enables or disables Emergency Management Services (EMS) for a specified boot application
- ▶ **/ems:** Enables or disables EMS for an operating system boot entry
- ▶ **/emssettings:** Specifies global EMS parameters
- ▶ **/store:** Specifies the BCD store upon which a command acts

To set a new default boot volume, run the following command:

```
bcdedit /default id
```

where the *id* is the identifier for the new entry.

For example, to configure the Windows Boot Manager to start the previous installation of Windows XP by default (which is identified as `{ntldr}`), run the following command:

```
bcdedit /default {ntldr}
```

To configure the currently running instance of Windows 7 as the default, run the following command:

```
bcdedit /default {current}
```

To change the timeout on showing boot menu:

```
bcdedit /timeout 5
```

To change the title of the boot menu entry, you would use the `/set` option. For example, to change the title to Windows XP from Earlier Windows Version, you would type in the following:

```
bcdedit /set {ntldr} description "Windows XP"
```

For more information about the `bcdedit` command, visit the following websites:

[http://technet.microsoft.com/en-us/library/cc709667\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc709667(WS.10).aspx)

<http://www.windows7home.net/how-to-use-bcdedit-in-windows-7>

## Enabling a Dual-Boot System

Sometimes, it might be beneficial to have a single computer have the capability to boot more than one operating system so that you can save on purchasing additional hardware or when you want to test a new operating system. You can configure a computer to boot different copies of Windows, each of which is selected during a Windows boot menu.

If you want to have Windows 7 on the same system as Windows XP, you need to install Windows XP first while leaving room on the same drive or a different drive on the computer to install Windows 7. Then, install Windows 7 using the custom installation and select the partition on which you want to install Windows 7. Windows 7 automatically identifies your previous installation of Windows (XP) and includes it in the boot menu.

To create a dual-boot system between Windows Vista and Windows 7 (or multiple copies of Windows Vista and Windows 7), the procedure is very similar to creating a dual boot system with Windows XP and Windows 7. One difference when you have a Windows Vista or Windows 7 installation is that you can use the Disk Management console (found as part of the Computer

Management console) to shrink a volume if you have free disk space on the volume you want to shrink. It is usually recommended that you defrag the hard drive first. Then right-click the volume you want to shrink and select **Shrink Volume**. After you've allocated the desired amount of space, click the **Shrink** button. Windows creates a new partition out of the free space you've allocated, all without even having to reboot. Of course, because this is a major change to the system, you should make sure that you have a good backup of your data before shrinking the volume.

You can also modify the default operating system and the time the list of operating system appears by right-clicking **Computer**, selecting **Properties**, clicking **Advanced system settings**, selecting the **Advanced** tab, and clicking the **Settings** button in the Startup and Recovery section. You can also specify what type of dump occurs during a system failure.

---

## Cram Quiz

1. Which versions of Windows can be directly upgraded to Windows 7 Home Premium Edition?
  - A. Microsoft Windows XP Professional
  - B. Microsoft Windows XP Home
  - C. Microsoft Windows XP Tablet PC
  - D. Microsoft Windows 2000 Professional SP3
  - E. None of the above
2. You work as a helpdesk technician for Acme.com. You have a Windows XP computer that you need to upgrade to Windows 7, but you are not sure if the older sound card and video card are compatible? What should you do?
  - A. Run the Windows 7 Program Compatibility Assistant tool
  - B. Run the Windows 7 Upgrade Advisor
  - C. Run the Windows Update
  - D. Open the Device Manager and update its drivers
3. What command or utility do you use to configure BCD store, add boot menu options, and change the default boot operating system?
  - A. System Configuration
  - B. `bcdedit`
  - C. Computer Management Console
  - D. Windows Boot Manager Console

## Cram Quiz Answers

1. **E** is correct. You cannot upgrade Windows XP or Windows 2000 Professional to Windows 7 Home Premium. Therefore, A, B, C, and D are incorrect.
  2. **B** is correct. When you want to determine system compatibility with Windows 7, you should run the Windows 7 upgrade Advisor. Answer A is incorrect because it does not check hardware compatibility. Answer C is incorrect because Windows update does not specify if a device is compatible with Windows 7. Answer D is incorrect because updating drivers in Windows XP does not specify if a device is compatible with Windows 7.
  3. **B** is correct. `bcdedit` is a command-line tool for managing BCD stores. It can be used for a variety of purposes, including creating new stores, modifying existing stores, adding boot menu options, and so on. Answer A is incorrect because System Configuration is used to manage startup programs and services. Answer C is incorrect because the Computer Management Console includes multiple management tools including the Disk Management MMC, but it does not have any tools to manage the BCD stores. Answer D is incorrect because the Windows Boot Manager is a Windows boot component. It is not a console or tool to configure the Windows BCD stores.
-

# Windows Easy Transfer and Windows User State Migration Tool

- ▶ Migrate user profiles.

## CramSaver

1. What are the two tools used to migrate user settings between a Windows Vista computer and Windows 7? (Choose two answers.)
  - A. Windows migrate.exe tool
  - B. Windows Easy Transfer
  - C. Windows User State Migration Tool
  - D. Windows Disk Migration Tool
2. If you want to migrate user settings from a Windows XP computer, which parameter should you use with the `ScanState.exe` command?
  - A. `/xp`
  - B. `/target:xp`
  - C. `/targetxp`
  - D. No options are required.

## Answers

1. **B** and **C** are correct. Both the Windows Easy Transfer and Windows User Migration Tool can migrate user settings between one Windows computer to another. Although the Windows Easy Transfer is used for a small number of migrations, the User State Migration Tool is a scriptable command-line tool that should be used for large deployments. Answers A and D are invalid and therefore incorrect.
2. **C** is correct. When you want to migrate from a Windows XP computer, you should use the `/targetxp` parameter. Answers A and B have invalid syntax and are therefore incorrect. Answer D is incorrect because C is a valid parameter.

If you cannot do an in-place upgrade, you can still move your data files and settings from one Windows installation (Windows XP, Windows Vista, and Windows 7) to another or from one computer running Windows to another using the Windows Easy Transfer (WET) program or the User State Migration Tool (USMT).

WET is a graphical program that enables you to transfer one user's profile or multiple users' profiles. You cannot use WET to move program files and you cannot transfer any system files such as fonts and drivers. With WET, you can transfer files and settings using a network, a USB flash drive (UFD), or the Easy Transfer cable; however, you cannot use a regular universal serial bus (USB) cable to transfer files and settings using WET. You can purchase an Easy Transfer cable on the Web, from your computer manufacturer, or at an electronics store.

WET (Migwiz.exe) is installed with Windows 7 and is located under **Accessories, System Tools**. It is also available on the Windows 7 DVD in the Support\Migwiz directory.

The User State Migration Tool (USMT) is a scriptable command-line tool that is highly customizable. Because it is a scriptable command-line tool, it is usually used to automate migration during large deployments of the Windows operating system.

USMT has been around for several years.

- ▶ USMT 2.0 was made to migrate to Windows 2000 and Windows XP workstations. USMT 2.6.2 was made available publicly.
- ▶ USMT 3.0 was made to migrate to Windows XP and Windows Vista. It also migrated EFS files and certificates. USMT 3.01 was made available publicly.
- ▶ USMT 4.0 was made to migrate to Windows Vista and Windows 7. It is included in the Windows Automated Installation Kit.

USMT includes two components, ScanState and LoadState, and a set of modifiable .xml files:

- ▶ **MigApp.xml**: Used to migrate application settings to computers running Windows 7
- ▶ **MigUser.xml**: Used to migrate user folders, files, and file types to computers running Windows 7
- ▶ **MigDocs.xml**: Used to migrate all user folders and files that are found by the MigXmlHelper.GenerateDocPatterns helper function

In addition, you can use the config.xml file to exclude components from the migration with the **ScanState.exe /genconfig** option.



The **ScanState** command is used to scan the source computer, collect files and settings, and create a store. For example:

```
scanstate \\fileserver\share\mystore /x:migsys.xml /x:migapp.xml  
/x:miguser.xml /v:13
```

The **/v:13** option enables verbose, status, and debugger output.

You can also add the following options to the preceding command:

- ▶ **/efs:copyraw**: Used to migrate the EFS-encrypted files and EFS certificates.
- ▶ **/encrypt /key:keystring**: Encrypts the store with the specified key.
- ▶ **/l**: Specifies the location and name of the ScanState log.
- ▶ **/nocompress**: Disables compression of data and saves the files to a hidden folder called “File.” Compression is enabled by default.
- ▶ **/p**: Without any additional parameters gives you storage space estimation if used with the **/nocompress** option.
- ▶ **/targetvista**: Use this option if you are migrating from a Windows Vista computer.
- ▶ **/targetxp**: Use this option if you are migrating from a Windows XP.
- ▶ **/vsc**: Enables the volume’s shadow-copy service to migrate files that are locked or in use.

### ExamAlert

**/efs:copyraw** began with USMT 3.0, which is used to copy encrypted EFS files and its certificates.

The **LoadState** command migrates the files and settings from the store to the destination computer. The **LoadState** command has similar options. Of course instead of using the **/encrypt** option to encrypt the store, you would use the **decrypt** option to decrypt the store.

No matter which program you decide to use, WET or USMT, you generally follow the same high-level steps to migrate user settings from one computer to another. These steps include the following:

1. Verify that your system is capable of running of Windows 7 by using the Windows 7 Upgrade Advisor. You also need to determine which applications have compatibility problems with Windows 7 and resolve those compatibility issues.
2. To protect from data loss, make sure to back up any data and personal settings before you start the upgrade.
3. Run WET or USMT to copy user profiles to a network drive or removable drive.
4. Install Windows 7 and perform a clean installation.
5. Use the Microsoft update site to update Windows with the newest patches, fixes, and security packs.
6. Re-install all programs.
7. Use WET or USMT 4.0 to migrate both your program settings and your user-related settings from the network or removable drive to complete the migration process.

For more information about Easy Transfer and USMT, visit the following website:

[http://technet.microsoft.com/en-us/library/ee461274\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee461274(WS.10).aspx)

---

## Cram Quiz

1. Which command would you use with the USMT to copy user profiles from a source computer?
  - A. scanstate
  - B. loadstate
  - C. copystate
  - D. migstate

2. You need to migrate the user settings from Windows XP Professional workstations to Windows 7 Enterprise workstations. Because some users use EFS, you need to also migrate the EFS files and certificates. You also need to ensure that you are able to encrypt the migration store during the migration. What should you use?
- A. On the Windows XP computers, use the USMT 3.0.
  - B. On the Windows XP computer, use the USMT 2.6.
  - C. On the Windows XP computer, use the EFSCopy command.
  - D. On the Windows XP computer, use the Export certificates using the Certificates MMC console. Be sure to select the Export file option.

## Cram Quiz Answers

1. **A** is correct. To migrate data from a source computer to a network or removable disk, you use `scanstate` to create a store. When the target computer is ready, you then use `loadstate` (Answer B) to migrate the data to the target. Answers C and D are incorrect because the `copystate` and `migstate` commands are not included with Windows 7.
  2. **A** is correct. The `/efs:copyraw` option specifies to copy the files in the encrypted format. This option was introduced with USMT 3.0; therefore, you need to use USMT 3.0 or higher. Answer B is incorrect because USMT 2.6 did not support migrating EFS files. Answer C is incorrect because the EFSCopy command does not exist. Answer D is incorrect because there is no Export File option and using the Certificates MMC console does not move files over.
-

# Deploying Windows 7

- ▶ **Deploying Windows 7:**
  - ▶ **Capture a system image**
  - ▶ **Prepare a system image for deployment**
  - ▶ **Deploy a system image**
  - ▶ **Configure a VHD**

## CramSaver

1. You want to establish an automated installation of Windows 7 using the Microsoft Windows 7 DVD. What should you do?
  - A.** Create an answer file called `oobe.xml` in the `C:\` folder of the computer
  - B.** Create an answer file called `winnt.sif` file and copy it to a USB drive
  - C.** Create an answer file called `autounattend.xml` in the `C:\` folder of the computer
  - D.** Create an answer file named `autounattend.xml` and copy it to a USB drive
2. You have an offline Windows 7 image. What tool would you use to add updated device drivers to the image?
  - A.** Use the `imagex` command-line utility
  - B.** Use the `pkgmgr.exe` utility
  - C.** Use Windows SIM
  - D.** Use the DISM tool

## Answers

1. **D** is correct. To perform an automated installation of Windows 7, the installation process automatically looks for the `autounattend.xml` file on the DVD or USB drive. Answer A is incorrect because the `oobe` is an option to use with `sysprep`, not an answer file. Answer B is incorrect because the `winnt.sif` file is an answer file used in older versions of Windows. Answer C is incorrect because the `autounattend.xml` file needs to be put on a USB drive or network drive, not the `C:\`.
2. **D** is correct. Deployment Image Servicing and Management (DISM) is a command-line tool that is used to service and manage Windows images. You can use it to install, uninstall, configure, and update Windows features, packages, drivers, and international settings. Answer A is incorrect because `imagex` is used to create and manage a WIM file. Answer B is incorrect because `pkgmgr.exe` (short for Package Manager) installs, uninstalls, configures, and updates features and packages for Windows. Answer C is incorrect because Windows SIM is used to create or validate answer files.

When you are at home and you need to install a single copy of Windows 7, it is simple enough to boot with the Windows 7 DVD and perform the installation. But when you are with a corporation and you need to perform hundreds of installations, it becomes a bit more challenging to install numerous machines while keeping the machines standardized. Therefore, Microsoft offers several ways to deploy Windows 7.

## Windows Automated Installation Kit

The Windows Automated Installation Kit (AIK) is a set of tools and documentation that support the configuration and deployment of Windows operating systems. By using Windows AIK, you can automate Windows installations, capture Windows images with ImageX, configure and modify images using Deployment Imaging Servicing and Management (DISM), create Windows PE images, and migrate user profiles and data with the User State Migration Tool (USMT). Windows AIK also includes the Volume Activation Management Tool (VAMT), which enables IT professionals to automate and centrally manage the volume activation process using a Multiple Activation Key (MAK).

If you have older systems that do not have DVD drives but do have CD-ROM drives, you can use the `createspannedshares.cmd` script to create spanned media, which then divides the DVD into multiple CDs. The `createspannedshares.cmd` is part of the Windows AIK.

To install the Windows AIK, you must first download the ISO, write the ISO file to a DVD using a third-party tool, and then install the Windows AIK from the DVD. The Windows AIK for Windows 7 can be found at the following website:

<http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en>

## Windows PE

Windows Preinstallation Environment (Windows PE or WinPE) is a light-weight version of Windows that is booted from a network disk, a CD, or a USB flash drive. Windows PE can be used to deploy workstations and servers, restore Windows to manufacturing specifications, and as a tool to fix and troubleshoot a wide variety of problems.

The newest version of Windows PE is Windows PE 3.0, which is built from Windows 7. To create a Windows PE disk, you would run the `copype.cmd` script and then copy the `imagex.exe` file to the iso folder under the

WinPE\_x86 directory. Next create the **wimscript.ini** configuration file in Notepad and save the file in the same directory as `imagex.exe`. Lastly, run the **oscdimg** command to create an ISO image of WinPE and burn the image to a CD. For more information, visit the following website:

[http://technet.microsoft.com/en-us/library/dd799303\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd799303(WS.10).aspx)

Windows PE 3.0 is available in both 32-bit and 64-bit versions. If you need to install a 32-bit version of Windows 7 using Windows PE, you must boot with the 32-bit version. If you need to install a 64-bit version of Windows 7, you must boot with the 64-bit version.

Original equipment manufacturers (OEMs) such as HP and Dell often include a system recovery disc rather than an operating system installation disc. The system recovery disk (which is sometimes a Windows PE disc) includes an image file so that you can boot with the disc and restore the computer to its original state as it left the manufacturer.

## Disk Cloning and the System Preparation Tool

One way to install Windows 7 is to use disk cloning software such as Norton Ghost to create an image file. To use the disk cloning software, you use the installation disc to install Windows onto a master computer (also called reference computer), update and patch the computer, customize Windows, and install any additional software. You then use the cloning software to copy the contents of a hard drive to a file. You use the disk cloning software to copy the contents of the image to a target computer.

If you create a cloned copy of Windows and apply the cloned copy to multiple computers, each copy of Windows cloned to a target computer using the same image has the same parameters, such as the same computer name and security identifier (SID). Unfortunately, for these computers to operate properly on a network, these parameters have to be unique.

To overcome this problem, you run the *System Preparation Tool (Sysprep)*, which removes the security identifiers and all other user-specific or computer-specific information from the computer before you run the disk cloning software to make the cloned disk image. When you copy the cloned image to the disk image, a small wizard runs that enables you to specify the computer name and other computer specific information. The SID and other information is re-created automatically. The Sysprep utility is located in the

c:\Windows\System32\sysprep or the c:\Windows\SysWOW64\sysprep folder. The disk structure is explained more in Chapter 9, “Managing Files and Folders.”

The syntax for the `sysprep` command is as follows:

```
sysprep.exe [/oobe | /audit] [/generalize] [/reboot | /shutdown | /quit] [/quiet] [/unattend:answerfile]
```

- ▶ **/audit:** Restarts the computer into audit mode. Audit mode enables you to add additional drivers or applications to Windows. You can also test an installation of Windows before it is sent to an end user. If an unattended Windows setup file is specified, the audit mode of Windows Setup runs the `auditSystem` and `auditUser` configuration passes.
- ▶ **/generalize:** Prepares the Windows installation to be imaged. If this option is specified, all unique system information is removed from the Windows installation. The security ID (SID) resets, any system restore points are cleared, and event logs are deleted. The next time the computer starts, a `specialize` configuration pass runs. A new security ID (SID) is created, and the clock for Windows activation resets, if the clock has not already been reset three times.
- ▶ **/oobe:** Restarts the computer into Windows Welcome mode. Windows Welcome enables end users to customize their Windows operating system, create user accounts, name the computer, and other tasks. Any settings in the `oobe` system configuration passed in an answer file are processed immediately before Windows Welcome starts.
- ▶ **/reboot:** Restarts the computer. Use this option to audit the computer and to verify that the first-run experience operates correctly.
- ▶ **/shutdown:** Shuts down the computer after Sysprep completes.
- ▶ **/quiet:** Runs Sysprep without displaying onscreen confirmation messages. Use this option if you automate Sysprep.
- ▶ **/quit:** Closes Sysprep after running the specified commands.
- ▶ **/unattend:answerfile:** Applies settings in an answer file to Windows during unattended installation. The *answerfile* specifies the path and filename of the answer file to use.

**ExamAlert**

If you are using a single image to install onto multiple computers, you need to use the `sysprep` command to strip the computer name and security ID and create a new computer name and security ID when you first start a computer with an image that was prepped.

## The Unattended Installation

An answer file is an XML file that stores the answers for a series of graphical user interface (GUI) dialog boxes. Because the answer file is an XML file, you can use any text editor, such as Notepad, to create and modify the answer file. However, you will find it much easier if you use the Windows System Image Manager.

If you call the answer file *autounattend.xml* and place in a USB flash drive, you can then perform an unattended installation just by rebooting the computer and booting from the Windows 7 installation DVD. Windows 7 setup (`setup.exe`) automatically searches the root directory of all removable media for an answer file called *autounattend.xml* and performs the installation without you replying to any prompts on the screen.

To see more information about basic Windows deployment, visit the following website:

[http://technet.microsoft.com/en-us/library/dd349348\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd349348(WS.10).aspx)

## Installing Windows Using Windows System Image Manager

Windows System Image Manager (Windows SIM) provides a GUI to create unattended Windows setup answer files. Using Windows SIM, you can:

- ▶ Create or update existing unattended answer files
- ▶ Validate the settings of an existing answer file against a WIM file
- ▶ View all the configurable component settings in a WIM file
- ▶ Create a configuration set
- ▶ Add third-party drivers, applications, or other packages to an answer file



**ExamAlert**

Although you can create an answer file using any text editor, it is recommended that you validate the answer file with the Windows System Image Manager.

To install Windows SIM, you first need to download and install Windows Automated Installation Kit (AIK) for Windows 7 from the Microsoft website. To start Windows SIM, you then click the **Start** button, select **Microsoft Windows AIK**, and select **Windows System Image Manager**.

To deploy Windows 7 by using ImageX, do the following:

1. Install and configure Windows 7 on a source PC.
2. Use **syprep** on the PC so that the OS can be deployed by removing some computer-specific information such as the workstation's SID, which must be unique.
3. Boot the master with the Windows PE CD.
4. Use ImageX on the master to create the image file.
5. Boot the target with the Windows PE CD.
6. Use Diskpart to format the drive. Diskpart is a PE tool that is used to configure the hard drive on a PC.
7. Use ImageX to apply the image to the target.

For more information, see the Windows 7 Upgrade and Migration Guide, located at the following website:

[http://technet.microsoft.com/en-us/library/dd446674\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd446674(WS.10).aspx)

## Deploying Windows with WIM Images

The Windows installation files can be distributed within a *Windows Imaging Format (WIM) file*. WIM is the file-based imaging format that Windows Server uses for rapid installation on a new computer. WIM files store copies (known as images) of the operating systems, such as Windows PE, Windows 7, or Windows Server 2008. Maintaining an operating system in a WIM file is easy because you can add and remove drivers, updates, and Windows components offline without ever starting the operating system.

The following are the benefits of using a file-based image format over the typical sector-based image format:

- ▶ A single WIM file deals with different hardware configurations.
- ▶ WIM can store multiple images within a single file.
- ▶ WIM enables compression and single instancing of files. Single instancing enables multiple images to share a single copy of a file.
- ▶ WIM allows images to be serviced offline. You can add or remove drivers, files, and patches.
- ▶ A WIM image can be installed on partitions of any size, unlike sector-based image formats.
- ▶ WIM enables you to boot Windows PE from a WIM file.

You can do the following with WIM files:

- ▶ When installing Windows 7 using Windows Deployment Server (WDS), you first boot the system with Windows PE. You then install Windows 7 from a WIM file that contains the Windows image.
- ▶ You can mount the WIM image as a new volume under Windows with a drive letter associated to facilitate easier extraction.
- ▶ You can mount the WIM image as a new volume and convert the WIM image to an ISO image.
- ▶ WIM images can be made bootable, as is the case with the setup DVD for Windows 7. In this case, `BOOT.WIM` contains a bootable version of Windows PE from which the installation is performed. Other setup files are contained in the file `INSTALL.WIM`.
- ▶ Because Windows PE can be contained within a WIM file, you can start Windows PE directly from a WIM file without copying it to a hard disk.

The image-based installation process consists of five high-level steps. These steps include the following:

1. Build an answer file, which is used to configure Windows settings during installation.
2. Build a reference installation with a customized/configured installation of Windows that you plan to duplicate onto one or more destination computers.

3. Create a bootable Windows PE media by using the `copype.cmd` script so that you can start a computer for the purposes of deployment and recovery.
4. Capture the Installation Image of the reference computer by using Windows PE and the ImageX tool. You can store the captured image on a network share.
5. Deploy the image from a network share onto a destination computer by using Windows PE and ImageX technologies. Follow these steps to deploy the image from a network share:
  - a. Start the computer by using Windows PE media.
  - b. Format that hard drive.
  - c. Connect to your network share and copy the custom image down to the destination computer's local hard drive.
  - d. Apply the image by using ImageX.

For high-volume deployments, you can store the image of the new installation to your distribution share and deploy the image to destination computers by using deployment tools, such as Windows Deployment Services (WDS) or Microsoft Deployment Toolkit (MDT).

To create and manage a WIM file, you use the ImageX command-line tool, which is available in several of Microsoft's deployment tools, such as in the Windows Automated Installation Kit (WAIK), Windows OEM Preinstallation Kit (OPK), or in Business Desktop Deployment 2007. By using the ImageX command-line tool, you can do the following:

- ▶ View the contents of a WIM file
- ▶ Capture desktop images
- ▶ Mount images for offline image editing
- ▶ Store multiple images in a single file
- ▶ Compress image files
- ▶ Implement scripts for image creation

The `imagex` command uses the following syntax:

```
imagex [flags] {/append | /apply | /capture | /delete | /dir |  
/export  
| /info | /mount | /mounttrw | /split | /unmount} [parameters]
```

- ▶ **/append:** Used to add a volume image to an existing WIM file and create a single instance of the file.
- ▶ **/apply:** Used to apply a volume image to a specified drive.
- ▶ **/capture:** Used to capture a volume image from a drive to a new .wim file.
- ▶ **/delete:** Used to remove the specified volume image from a .wim file.
- ▶ **/dir:** Displays a list of the files and folders within a specified volume image.
- ▶ **/export:** Exports a copy of the specified .wim to another .wim file. If you use the `/ref splitwim.swm` option, it enables you to reference a split .wim file (`*.swm`).
- ▶ **/info:** Returns information about the WIM file.
- ▶ **/mount:** Used to mount a WIM file with read-only permission.
- ▶ **/mountw:** Used to mount a WIM file with read/write permission, thereby allowing the contents of the file to be modified.
- ▶ **/split:** Splits an existing .wim file into multiple read-only split .wim files (`*.swm`).
- ▶ **/unmount:** Used to unmount an image from a specified directory.

The *parameters* options vary based on the options that you select. For example, you can use several parameters when you use the `/append` option; you can use the `/boot` parameter to mark the volume image as bootable; and use the `/check` parameter to check the integrity of the WIM file.

For more information about the `imagex` command, visit the following website:

<http://msdn.microsoft.com/en-us/library/ff794852.aspx>

## Deployment Image Servicing and Management

Deployment Image Servicing and Management (DISM) is a command-line tool that is used to service and manage Windows images. You can use it to install, uninstall, configure, and update Windows features, packages, drivers, and international settings.

DISM can also be used to service Windows PE images. DISM is installed with Windows 7 and is also distributed in Windows OPK and Windows AIK. It is a consolidated tool that replaces several tools such as PEimg, Intlcfg, and Package Manager used in Windows, with added functionalities to improve the experience for offline servicing.

You can use DISM to:

- ▶ Add, remove, and enumerate packages and drivers
- ▶ Enable or disable Windows features
- ▶ Apply changes based on the `offlineServicing` section of an `unattend.xml` answer file
- ▶ Configure international settings
- ▶ Upgrade a Windows image to a different edition
- ▶ Prepare a Windows PE image
- ▶ Take advantage of better logging
- ▶ Service all platforms (32-bit, 64-bit, and Itanium), service a 32-bit image from a 64-bit host, and service a 64-bit image from a 32-bit host
- ▶ Use old Package Manager Scripts

The base syntax for nearly all DISM commands is the same. After you have mounted or applied your Windows image so that it is available offline as a flat file structure, you can specify any DISM options, the servicing command that updates your image, and the location of the offline image. You can use only one servicing command per command line. If you are servicing a running computer, you can use the `/Online` option instead of specifying the location of the offline Windows Image.

The base syntax for DISM is the following:

```
DISM.exe {/Image:path_to_image | /Online} [dism_options]
[servicing_command] [servicing_argument]
```

The following DISM options are available for an offline image:

```
DISM.exe /image:path_to_offline_image_directory
[/WinDir:path_to_%WINDIR%] [/LogPath:path_to_log_file.log]
[/LogLevel:n] [SysDriveDir:path_to_bootMgr_file] [/Quiet]
[/NoRestart] [/ScratchDir:path_to_scratch_directory]
```

The following DISM options are available for a running operating system:

```
DISM.exe /online [/LogPath:path_to_log_file] [/LogLevel:n] [/Quiet]
[/NoRestart] [/ScratchDir:path_to_scratch_directory]
```

Before you start working with an image, you need to retrieve information about the OS images that are contained within a WIM file. Do this with the following command:

```
dism /Get-WimInfo /WimFile:d:\sources\install.wim
```

If you add the command-line option **/index** plus the image's index number, you get information about a specific image, such as the OS version, size, installed service pack, and so on:

```
dism /Get-WimInfo /WimFile:d:\sources\install.wim /index:4
```

Before you can work with a WIM image, you have to mount it to a folder with the following command:

```
dism /Mount-Wim /wimfile:c:\wim\install.wim /index:4 /MountDir:c:\img
```

If you need to mount an image onto a DVD or if you want to access the image in read-only mode, you just have to add **/ReadOnly** to the command.

After you have mounted an image, you can navigate through its folder structure using Windows Explorer and make changes to all files and folders. In most cases, however, you use DISM to gather specific information about an image and also to add features, drivers, and packages.

To list all installed third-party drivers in the image mounted to *c:\img*, you execute the following command:

```
dism /image:c:\img /Get-Drivers
```

To add the driver (INF) file to the image in the mount directory, you execute the following command:

```
dism /image:c:\img /add-driver /driver: C:\drivers\driver.INF
```

To dismount the image, execute the following command:

```
dism /unmount-wim /mountdir:c:\img /discard
```

For more information about the Deployment Image Servicing and Management program, visit the following websites:

[http://technet.microsoft.com/en-us/library/dd744256\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744256(WS.10).aspx)

[http://technet.microsoft.com/en-us/library/dd744382\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd744382(WS.10).aspx)

## Windows Deployment Services

Another way to install Windows is to use the Windows Deployment Services (WDS). You can use it to deploy Windows Vista, Windows 7, and Windows Server 2008. By booting a computer with Windows PE 2.0 or 3.0, you can connect to the WDS server and install Windows from a configured image.

If you choose to install the Deployment Server, you need the following prerequisites available on your network:

- ▶ Active Directory Domain Services
- ▶ Dynamic Host Configuration Protocol (DHCP) server
- ▶ Dynamic Name Services (DNS) server

Unfortunately, installing and configuring the Windows Deployment Services is beyond the scope of this exam.

To install Windows 7 using a Windows Deployment Server, you would

1. Turn on your computer and boot from the network card (PXE).
2. By booting using PXE, you connect to the Windows Deployment Service server and download the customized Windows PE image across the network.
3. The new computer loads Windows PE into memory and launches the configuration script. The script verifies the computer's configuration and hardware requirements.
4. If necessary, the script backs up the user's data to a shared folder on another computer.
5. The script runs the Diskpart tool to partition and format the disk.

The script connects to a shared folder containing the Windows Setup files and runs the Windows Setup program to install the operating system fully unattended.

---

## Cram Quiz

1. You manually create an answer file for a Windows 7 unattended installation. What should you do next?
  - A. Use `sysprep.exe` to capture an image on a reference computer
  - B. Use `imagex.exe` to capture an image on a reference computer
  - C. Use Windows SIM to validate the answer file
  - D. Use `sysprep.exe` to validate the answer file
2. What tool can you use to create a bootable media that is used to deploy Windows 7 on non-PXE-supporting client computers?
  - A. Use Windows SIM
  - B. Use Windows AIK
  - C. Use BDD
  - D. Use SMS

## Cram Quiz Answers

1. **C** is correct. Although you can create an answer file with any text editor, it is recommended that you use Windows SIM to validate the answer file. Answer A is incorrect because `sysprep.exe` is used to prepare a system for mass deployment by removing the security identifiers and all other user-specific or computer-specific information from the Windows volume before cloning. Answer B is incorrect because `imagex.exe` is used to create and manage WIM files. Answer D is incorrect because Windows SIM is used to validate the answer file.
  2. **B** is correct. To create bootable media to deploy Windows 7 on non-PXE-supporting client computers, you need create a WinPE disk, which is done with Windows Automated Installation Kit (AIK). Answer A is incorrect because Windows SIM is used to create and validate answer files. Answer C is incorrect because Business Desktop Deployment (BDD) was a deployment tool mostly used with deploying Windows, but does not include tools to create a WinPE disk. Answer D is incorrect because SMS (short for System Management Server) has been replaced with System Center Configuration Manager to deploy and manage operating systems, patches, and software. It does not help boot a system that cannot PXE boot.
-



# Booting with a VHD Image

## ► Configure a VHD

### CramSaver

1. When using a virtual system such as Hyper-V, the disk for a virtual system is stored in what file?
  - A. VMC
  - B. VHD
  - C. VSV
  - D. AVHD
2. What utility would you use to create a VHD file?
  - A. bcdboot
  - B. bcdedit
  - C. imagex.exe
  - D. Disk Management console.

### Answers

1. **B** is correct. The virtual hard disk (.vhd) files store guest operating systems, applications and data for the virtual machine. Answer A is incorrect because the virtual machine configuration (.vmc) file contains the virtual machine configuration information including all settings for the virtual machine. Answer C is incorrect because the saved-state (.vsv) file is used if a virtual server has been placed in a saved state. Answer D is incorrect because the .avhd file is a differencing disk used with Hyper-V.
2. **D** is correct. To create a VHD, you would use the Disk Management console. Answer A is incorrect because `bcdboot` is a command-line tool for initializing the BCD store and copying boot environment files to the system partition. Answer B is incorrect because `bcdedit` is a command-line tool for managing Boot Configuration Data (BCD) stores. Answer C is incorrect because `imageX.exe` is a tool used to create and manage WIM files.

Over the last few years, virtualization has become popular. *Virtual machine* technology enables multiple operating systems to run concurrently on a single machine. This allows for a separation of services while keeping cost to a minimum. In addition, you can easily and quickly create Windows test environments in a safe, self-contained environment. Of course, for a virtual machine to handle such a load, it must have sufficient processing and memory resources.

Previously, Microsoft virtual server included Microsoft Virtual Server and Virtual PC. Starting with Windows Server 2008, Microsoft introduced *Hyper-V*. Hyper-V is based on *hypervisor*, a virtual machine monitor that provides a virtualization platform that allows multiple operating systems to run on a host computer at the same time. To keep each virtual server secure and reliable, each virtual server is placed in its own partition. A partition is a logical unit of isolation, in which operating systems execute.

Each virtual machine uses the following files:

- ▶ A *virtual machine configuration (.vmc) file* in XML format that contains the virtual machine configuration information, including all settings for the virtual machine.
- ▶ One or more *virtual hard disk (.vhd) files* to store the guest operating system, applications, and data for the virtual machine. So, if you create a 12 GB partition for the virtual machine's hard drive, the virtual hard disk file is 12 GB.

In Windows 7, a VHD can be used to store an operating system to run on a computer without a parent operating system, virtual machine, or hypervisor. This feature, called *VHD boot*, is a new feature in Windows 7 that eases the transition between virtual and physical environments. It is best used in the following scenarios:

- ▶ In an organization that has hundreds of users working remotely through Virtual Desktop Infrastructure (VDI) via virtual computers but also needs the same desktop images as the users working onsite using physical computers.
- ▶ In an organization with users in a highly managed environment that use technologies such as Folder Redirection and Roaming User Profiles so that the user state is not stored in the image.
- ▶ As dual boot, when you only have a single disk volume as an alternative to running virtual machines.

Windows 7 also enables IT professionals to use the same processes and tools to manage WIM and VHD image files.

The following steps outline Windows 7 deployment on VHD:

1. **Create the VHD:** You can create a VHD by using the DiskPart tool or the Disk Management MMC. The Disk Management MMC also enables you to attach the VHD, so that it appears on the host computer

as a drive and not as a static file. VHD files can then be partitioned and formatted before you install an operating system.

2. **Prepare the VHD:** Install Windows 7 on the VHD by using the **imagex** command with the **/capture** and **/apply** options.
3. **Deploy the VHD:** You can then copy the VHD file to one or more systems, to be run in a virtual machine or for native boot. To configure native-boot, add the native-boot VHD to the boot menu by using **bcdedit** or **bcdboot** tool. **bcdedit** is a command-line tool for managing Boot Configuration Data (BCD) stores and **bcdboot** is a command-line tool for initializing the BCD store and copying boot environment files to the system partition. You can also automate the network deployment of VHD by using WDS. You can use WDS to copy the VHD image to a local partition and to configure the local Boot Configuration Data (BCD) for native-boot from the VHD.

To create a VHD using the Disk Management console, perform the following instructions:

1. In the left pane, right-click **Disk Management** and then click on **Create VHD**. See Figure 2.5.

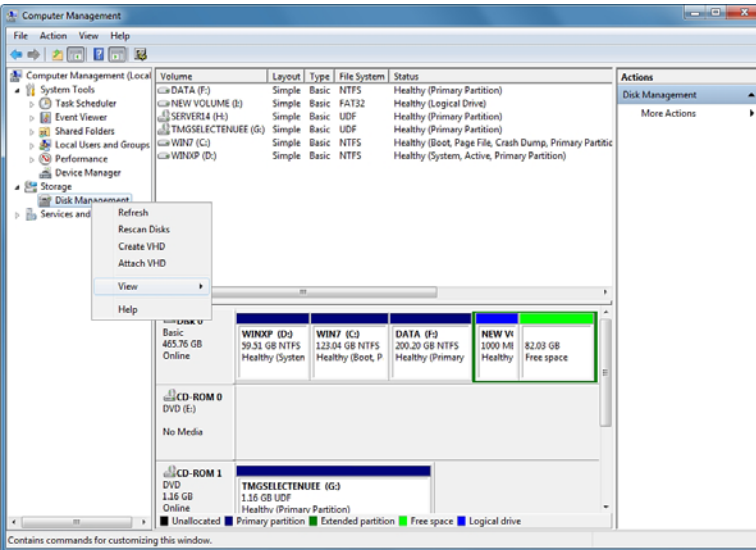


FIGURE 2.5 Using Disk Manager to create or attach a virtual hard disk.

2. After choosing to create a VHD, select a location to save your VHD file.
3. Next, enter the maximum size you want the Virtual Hard Disk to be, and select the size type to be used. Choose MB, GB, or TB (see Figure 2.6).

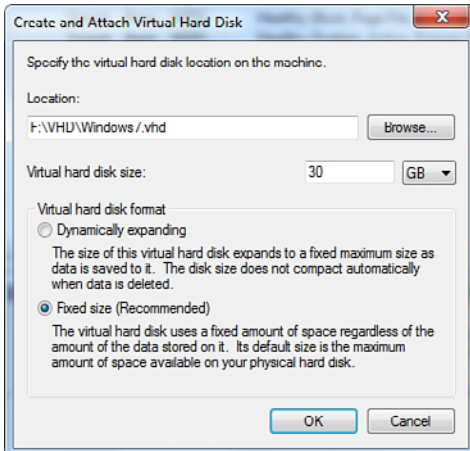


FIGURE 2.6 Specifying the location and size of the virtual hard disk.

4. Select whether to let Windows decide the size by choosing **Dynamic** or use a set size by choosing **Fixed** and clicking **OK**.
5. The new disk displays in the right pane as unallocated space. Right-click the new unallocated VHD Disk # and click **Initialize Disk**.
6. Select the **Disk #** from Step 5 for the new VHD. You have to choose if you want the new VHD to have Master Boot Record (MBR) or GUID Partition Table (GPT) partition and click **OK**.
7. Right-click the new unallocated VHD and click **New Simple Volume**.
8. Type the maximum disk space you want to use for this VHD partition and then click **Next**.
9. Select a FAT or a NTFS file system and enter a name for your VHD. Click the **Perform a quick format** checkbox and click **Next**.
10. When the summary appears, click the **Finish** button and the Disk Management console creates a new simple volume on your VHD, which is already attached.

You can also create a VHD using an open-source tool available on the MSDN Code Gallery called WIM2VHD, which converts the WIM image into a VHD you can use to boot off. You can find it at <http://code.msdn.microsoft.com/wim2vhd/>.

To install a VHD boot machine:

1. Boot the system with a Windows 7 DVD or USB flash drive.
2. At the setup screen, instead of choosing **Install Now**, press **Shift+F10** to get into command-line mode.
3. Enter `diskpart` to start the partitioning utility.
4. Create a new VHD file by entering the following command:

```
create vdisk file="d:\path_to-vhd.vhd" type=expandable
maximum=maxsizeInMegabyte
```

5. To select the new VHD and attach it as a physical disk, enter the following command:

```
select vdisk file="D:\pathToVhd.vhd"
```

6. Use **Alt+Tab** to switch back to the setup screen and start the setup to the attached VDisk.
7. Now proceed with the normal setup.
8. After the installation, Windows 7 displays in the boot menu. If you want to add a VHD manually to the boot menu, use this command sequence:

```
bcdedit /copy {originalguid} /d "New Windows 7 Installation"
bcdedit /set {newguid} device vhd=[D:]\Image.vhd
bcdedit /set {newguid} osdevice vhd=[D:]\Image.vhd
bcdedit /set {newguid} detecthal on
```

9. Open the Computer Management console and open Disk Management.
10. Right-click **Disk Management** and then click **Attach VHD**.

---

## Cram Quiz

1. You have a Virtual Hard Disk with Windows 7. How do you add the VHD to the Windows 7 boot menu?
  - A. Use `diskpart.exe` to select vdisk
  - B. Attach to your machine using Disk Management
  - C. Use the `bcdedit.exe` command and modify the Windows Boot Manager settings
  - D. Use the `bootcfg.exe` command to modify the Windows Boot Manager settings
2. What utilities do you use to create a VHD file? (Choose all that apply.)
  - A. `diskpart`
  - B. Disk Management
  - C. `bcdedit`
  - D. `bcdboot`

## Cram Quiz Answers

1. **C** is correct. For Windows Vista and 7, the boot menu is configured using the `bcdedit` command, which edits a hidden file called `c:\boot\bcd`. To add a VHD manually to the boot menu, you also use `bcdedit.exe`. Answer A is incorrect because `diskpart` is a PE tool that is used to configure the hard drive on a PC. Answer B is incorrect because adding a machine using Disk Management does not add Windows 7 running on a VHD to the boot menu. Answer D is incorrect because `bootcfg.exe` is used to modify the `boot.ini` on Windows Server 2003 machines.
  2. **A** and **B** are correct. `diskpart` and Disk Management are used to create a VHD file (virtual hard drive). Answer C is incorrect because `BCDedit` is used to configured using the `bcdedit` command, which edits a hidden file called `c:\boot\bcd` that displays the boot menu. To add a VHD manually to the boot menu, you would also use the `bcdedit.exe` utility. Answer D is incorrect because `bcdboot` is a command-line tool for initializing the BCD store and copying boot environment files to the system partition.
-

## Review Questions

1. You work as a desktop support technician at Acme.com. Because you need to connect to the domain, you need to install Windows 7 Enterprise Edition on a new computer for the graphics department. The new computer has the following specifications:
  - ▶ 1.4 GHz Intel processor
  - ▶ 512 MB of RAM
  - ▶ 50 GB hard drive
  - ▶ Super VGA video card with 256 MB of video memory
  - ▶ Integrated sound card
  - ▶ Intel 10/100 network adapter

Which hardware does not meet the minimum requirements to install Windows 7?

- A. The processor
  - B. The amount of RAM
  - C. The hard drive
  - D. The video card
  - E. The network adapter
2. You work as the desktop support technician at Acme.com. You have a computer that has a 120 GB hard drive divided into two partitions. Each partition is 60 GB. Windows XP Professional has been installed on the first partition. The second partition has not been defined. You want to set up the computer to dual boot between Windows XP Professional and Windows 7 Professional. What do you need to do to set this up?
    - A. Format the second partition with the NTFS file system. Boot from the Windows 7 DVD and install Windows 7 on the second partition.
    - B. Format the first partition with the NTFS file system. Boot from the Windows 7 DVD and install Windows 7 on the first partition.
    - C. Boot from the Windows 7 DVD and upgrade the Windows XP partition to Windows 7.
    - D. Install Windows XP on the first partition. Boot from the Windows 7 DVD and install Windows 7 on the second partition.
  3. You work as the desktop support technician at Acme.com. Within your corporation, you have new computer with Windows 7 Professional. You need to install the same build and configuration of Windows 7 on 10 other computers. To accomplish this, you burn a bootable Windows PE CD that includes all the required deployment tools. What should you do next with the least amount of administrative effort?

- A.** Boot the master with the Windows PE CD. Use ImageX on the master to create the image file. Boot each target with the Windows PE CD. Use Diskpart to format the drive. Use ImageX to apply the image to the target.
  - B.** Use Sysprep to seal the master. Boot the master with the Windows PE CD. Use ImageX on the master to create the image file. Boot each target with the Windows PE CD. Use ImageX to apply the image to the target.
  - C.** Boot the master with the Windows PE CD. Use ImageX on the master to create the image file. Boot each target with the Windows PE CD. Use Diskpart to format the drive. Use ImageX to apply the image to the target. Use Sysprep to seal the master.
  - D.** Use Sysprep to seal the master. Boot the master with the Windows PE CD. Use ImageX on the master to create the image file. Boot each target with the Windows PE CD. Use Diskpart to format the drive. Use ImageX to apply the image to the target.
4. You work as the desktop support technician at Acme.com. You have a new computer that has Windows XP on which you want to install Windows 7. You place the DVD into the drive and start the workstation. Unfortunately, it boots to Windows XP without starting the install program. You enter the BIOS program and determine that you are not allowed to boot from the DVD. What do you do next?
- A.** Install new drivers for the DVD drive
  - B.** Retrieve updates from Microsoft
  - C.** Update the PC's BIOS
  - D.** Boot from a Windows PE disk
5. Which versions of Windows can be upgraded to Windows 7 Home Premium Edition?
- A.** Microsoft Windows Vista Business
  - B.** Microsoft Windows Vista Home Basic
  - C.** Microsoft Windows Vista Starter
  - D.** Microsoft Windows Vista Ultimate
6. You have several workstations. You want to produce a new Security ID (SID) for each workstation. What should you do?
- A.** Using the Welcome screen, deactivate the license activation on all the Windows 7 workstations
  - B.** Use the System Properties and remove the computers from the domain



- C. Use the `sysinfo.exe /resetID` command on all the Windows 7 workstations
  - D. Use the `sysprep.exe /oobe /generalize` command on all the Windows workstations
7. You are going to migrate the server between two Windows 7 computers. You want to determine the amount of space needed to accomplish the migration. What should you do?
- A. Run the `scanstate` command with the `/nocompress /p` option on the source computer
  - B. Run the `scanstate` command with the `/nocompress /p` option on the target computer
  - C. Run the `loadstate` command with the `/nocompress /p` option on the source computer
  - D. Run the `loadstate` command with the `/nocompress /p` option on the target command
8. You manually create an answer file for a Windows 7 unattended installation. What can you use to validate the answer file?
- A. Use the Setup Manager
  - B. Use the Sysprep.exe utility
  - C. Use the Windows System Image Manager tool
  - D. Use `image.exe`
9. You want to create an image of a Windows 7 computer on multiple CDs. Therefore, you need to use the `createspannedshares.cmd` script. Where is the `createspannedshared.cmd` script found?
- A. The Package Manager
  - B. DISM
  - C. Windows AIK
  - D. Windows SIM
10. You have a system with both Windows Vista and Windows 7. Which command would you use to configure the system to start Windows Vista by default?
- A. Use the `bcdedit.exe` command with the `/default` option
  - B. Use the `bcdedit.exe` command with the `/Vista` option
  - C. Modify the `boot.ini` file to boot Vista using a text editor
  - D. Create the `boot.ini` in the C:\ folder and specify the `/Vista` option

# Review Question Answers

1. Answer **B** is correct. The system requirements specify a minimum of 1 GB of RAM. The other requirements are 15 GB hard drive space for the 32-bit edition, 20 GB hard drive space for the 64-bit edition, 1 GHz processor, and a video card with 128 MB of video memory. Therefore, Answers A, C, and D are incorrect. The system requirements do not specify a network card, so Answer E is not correct. Of course, you need a network card to communicate with a network.
2. Answer **A** is correct. To have a system dual boot between Windows XP and Windows 7, you have to install each operating system onto two different partitions. Because Windows XP is already on the first partition, you need to install Windows 7 on the other partition. You do not want to format the first partition because it erases everything on that partition. So, Answer B is incorrect. You don't want to upgrade Windows because Windows XP will not be available. Therefore, Answer C is incorrect. Answer D is incorrect because you don't need to install Windows XP; it already exists.
3. Answer **D** is correct. To install the same configuration on 10 different computers, you have to use images. You already have the source system. Answer D then specifies the rest of the steps to install Windows 7 with images. After you have the source computer, the next step would be to sysprep the system. Therefore, Answers A and C are incorrect. Because you need to create a new partition before installing the image, Answer B is incorrect.
4. Answer **C** is correct. Because the system did not find the DVD disc, you need to fix that problem. The BIOS not allowing you to specify a DVD to boot from indicates that the BIOS is too old to support bootable DVD drives. Therefore, you need to update the system BIOS. Answers A and B are incorrect because drivers and updates do not help boot from the DVD because these load when Windows 7 loads, and to boot from a DVD does not require Windows 7 to load. Answer D is incorrect because you don't need the Windows PE disk to load DVD drivers.
5. Answer **B** is correct. You can only upgrade from Windows Vista Home Basic and Windows Vista Home Premium to Windows 7 Home Premium. If you have Windows Vista Business, Windows Vista Starter, and Windows Vista Ultimate, you have to perform a custom install instead of an in-place upgrade. Therefore, A, C, and D are incorrect.
6. Answer **D** is correct. The System Preparation Tool (Sysprep) removes the security identifiers and all other user-specific or computer-specific information from the computer. Answers A and B are incorrect because the Welcome screen and the System Properties do not produce a new Security ID. Answer C is incorrect because `sysinfo.exe` does not have a `/resetID` option and cannot be used to reset the SID.
7. Answer **A** is correct. The `scanstate` command is used to scan the source computer, collect files and settings, and create a store. The `/p` option without any parameters gives you a storage space estimation if used with the `/nocompress` option. Answer C is incorrect because the `loadstate` command migrates the files and settings from the store to the destination computer.

Answers B and D are incorrect because you need to run the command on the source computer and not the target computer.

8. Answer **C** is correct. The Windows System Image Manager (Windows SIM) provides a GUI interface to create and validate unattended Windows setup answer files. Answer A is incorrect because the Setup Manager is a Windows XP deployment tool. Answer B is incorrect because the System Preparation Tool removes the security identifiers and all other user-specific or computer-specific information from the computer. Answer D is incorrect because `imagex.exe` is used to create and manage a WIM file.
9. Answer **C** is correct. If you have older systems that do not have DVD drives but do have CD-ROM drives, you can use the `createspannedshares.cdm` script to create spanned media, which then breaks the DVD to multiple CDs. The `createspannedshares.cdm` is part of the Windows AIK. Answer A is incorrect because `pkgmgr.exe` (short for Package Manager) installs, uninstalls, configures, and updates features and packages for Windows. Answer B is incorrect because the Deployment Image Servicing and Management (DISM) is a command-line tool that is used to service and manage Windows images including install, uninstall, configure, and update Windows features, packages, drivers, and international settings. Answer D is incorrect because the Windows System Image Manager (Windows SIM) provides a GUI to create or check unattended Windows setup answer files.
10. Answer **A** is correct. `bcdedit` is a command-line tool for managing Boot Configuration Data (BCD) stores. The `/default` option defines which operating system is the default boot operating system. Answer B is incorrect because you would not use a `/Vista` option. Answers C and D are incorrect because the `boot.ini` files are used in Windows XP boot menus, not for Windows Vista or 7 boot menus.

## CHAPTER 3

# System Management

**This chapter covers the following 70-680 Objectives:**

- ▶ Supplemental Objective: Manage and configure Windows
- ▶ Installing, Upgrading, and Migrating to Windows 7:
  - ▶ Configure devices
- ▶ Configuring Backup and Recovery Options:
  - ▶ Configure system recovery options

Now that you have learned how to installed Windows, you also need to know how to configure Windows, including installing devices. To configure and manage Windows, you still use the standard tools, including the Control Panel and Administrative Tools, which can be found in most modern versions of Windows. Although these tools have been updated, they still have a lot in common to these tools found in older versions of Windows.

# Configuring and Managing Windows

► Supplemental Objectives: Manage and configure Windows

## CramSaver

1. Which of the following is the primary tool to manage and configure Windows 7?
  - A. Registry Editor
  - B. Windows Explorer
  - C. Control Panel
  - D. System Manager
2. Which applet in the Control Panel do you use to change the computer name?
  - A. Name
  - B. System
  - C. Workgroup
  - D. Administrative Tools
3. What do you use to enable features so that disabled people can better use Windows 7? (Choose the best answer.)
  - A. Accessibility applet
  - B. Ease of Access Center
  - C. Administrative Tools
  - D. System applet

## Answers

1. **C** is correct. The primary program used to configure Windows is the Control Panel. Answer A is incorrect because the Registry Editor is used to manually change the registry, which should rarely be done. Answer B is incorrect because Windows Explorer is used to manage the files and folders. Answer D is incorrect because there is no System Manager that comes with Windows 7.
2. **B** is correct. To change the name of a computer to add the computer to a domain, you need to use the System applet in the Control Panel. Answers A and C are incorrect because there are no Name or Workgroup applets. Answer D is incorrect because Administrative Tools are more IT-oriented tools used in managing your computer.

3. **B** is correct. To configure accessibility options, you use the Ease of Access Center. Answer A is incorrect because the Accessibility applet was the name used in Windows XP. Answers C and D are incorrect because the Administrative Tools and System applet are not used for accessibility options.

To simplify the process of setting up a new computer, Windows 7 includes the Welcome Center/Getting Started screen, as shown in Figure 3.1. This screen pulls all the tasks you most likely want to complete when you set up your computer into a single location. Such tasks include adding user accounts for different people, transferring files and settings, backing up your files, personalizing Windows, and changing the size of the text on your screen. You can also use Homegroup to share files and printers with other computers in your home and go online to get Windows Live Essentials. You can also go online to find out what's new in Windows 7.



FIGURE 3.1 The Windows Welcome Center.

The *Control Panel* is a graphical tool used to configure the Windows environment and hardware devices, as shown in Figure 3.2. To access the Control Panel, you can click the **Start** button on the taskbar and select **Control Panel**. You can also display the Control Panel in any Windows Explorer view by clicking the leftmost option button in the Address bar and selecting **Control Panel**.

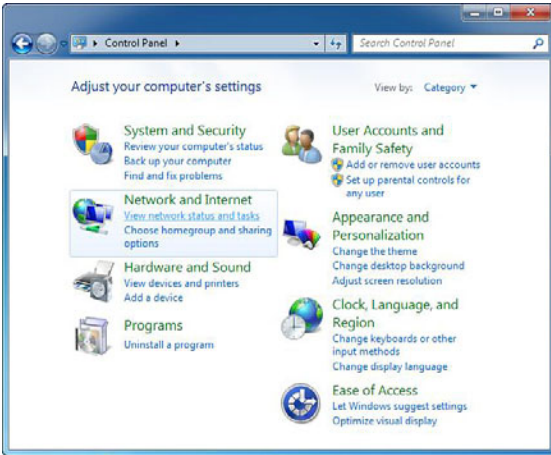


FIGURE 3.2 Windows 7 Control Panel in Category view.

Of the eight categories that are listed, each category includes a top-level link, and under this link are several of the most frequently performed tasks for the category. Clicking a category link provides a list of utilities in that category. Each utility listed within a category includes a link to open the utility, and under this link are several of the most frequently performed tasks for the utility.

As with Windows XP and Windows Vista, you can change from the default Category view to Classic view (Large Icon view or Small Icon view). Icon view is an alternative view that provides the look and functionality of Control Panel in Windows 2000 and earlier versions of Windows, as shown in Figure 3.3.

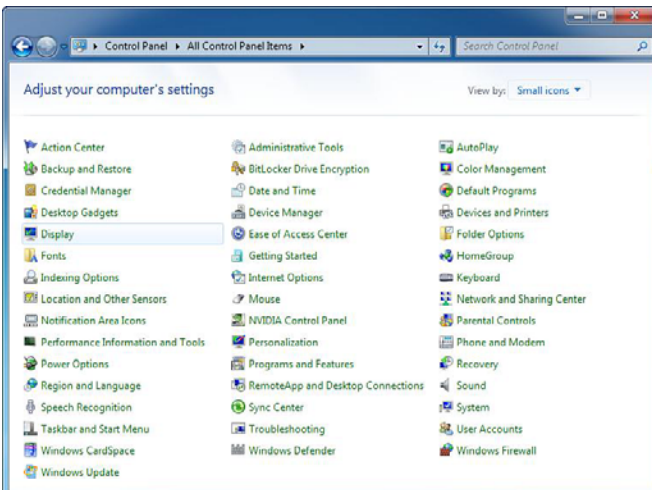


FIGURE 3.3 Windows 7 Control Panel in Small Icon view.

## Viewing Basic Information

You can view a summary of important information about your computer by opening System in Control Panel by clicking one of the following:

- ▶ If you are in Category view, click **System and Security** and click **View amount of RAM and processor speed**.
- ▶ If you are in Classic view, double-click the **System** applet.
- ▶ Right-click **Computer** and select **Properties**.

At the top of the screen, you see the Windows edition you have and the system type (32-bit or 64-bit) in the middle of the screen. Toward the bottom of the screen, you see the computer name and domain (if any), the Product ID, and if Windows is activated.

As Figure 3.4 shows, in the System section you find the Windows Experience Index (WEI) base score, which is a number that describes the overall capability of your computer. Your computer's processor type, speed, and quantity (if your computer uses multiple processors) are listed. For example, if your computer has two processors, you see "(2 processors)" displayed. Also displayed is how much random access memory (RAM) is installed and, in some cases, how much of the memory is usable by Windows.

### ExamAlert

To see the Windows 7 edition and version, open the System Properties.

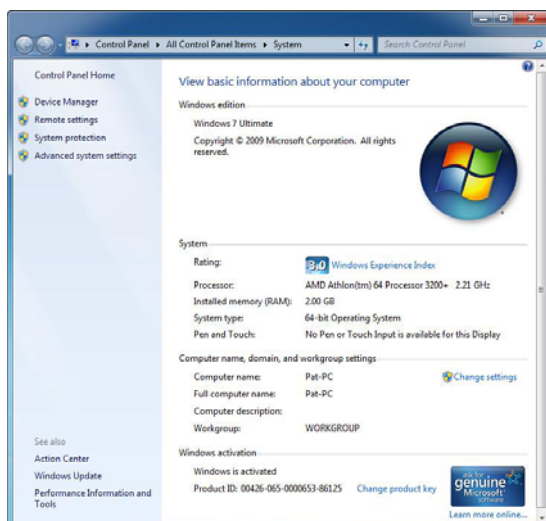


FIGURE 3.4 Computer properties.



## Changing Computer Name and Domain/Workgroup

Every computer should have a unique computer name assigned a network. To change the computer name, you open System in the Control Panel and click the **Change settings** option in the Computer name, domain, and workgroup settings section, which opens the System Properties dialog box, as shown in Figure 3.5. You then click the **Change** button and type in the computer name in the Computer name textbox.

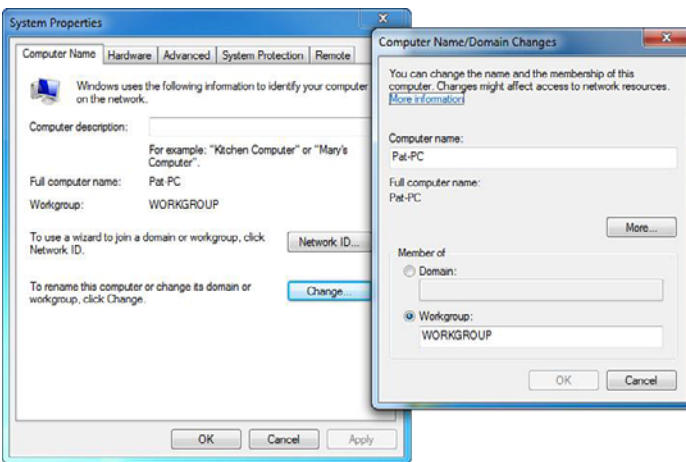


FIGURE 3.5 Changing computer name.

If you need to add a computer to a domain, you then select the Domain option, and specify the name of the domain in the Domain text box. When you click **OK**, you are asked for credentials for an administrative account for the domain. After you enter the credentials (username and password), it shows you a welcome dialog box. When you click **OK** to close the welcome dialog box and when you close the System Properties dialog box, you are prompted to reboot the computer.

To remove a computer from a domain, join an existing workgroup, or create a new workgroup, you select the workgroup option and type in the name of the workgroup. You then click **OK**. If you are removing yourself from the domain, you are asked for administrative credentials.

## Windows Features and Programs

Some programs and features included with Windows, such as Internet Information Services (IIS), must be turned on before you can use them. Other features might be on by default and you might want to turn them off if they are not going to be used. To turn on features, do the following:

1. Click **Programs** in the Control Panel.
2. Click **Turn Windows features on or off**.
3. In the screen shown in Figure 3.6, turn a feature on by selecting the checkbox next to the feature. To turn off a Windows feature, clear the checkbox.
4. Click **OK**.

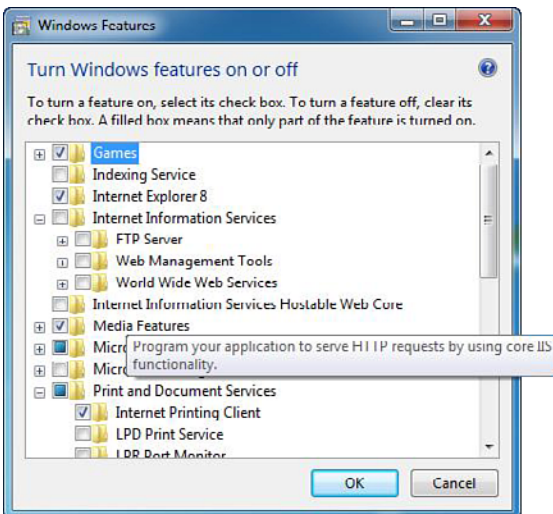


FIGURE 3.6 Turning Windows features on or off.

You can uninstall a program from your computer if you no longer use it or if you want to free up space on your hard disk. You can use Programs and Features to uninstall programs or to change a program's configuration by adding or removing certain options.

To uninstall a program or change a program, perform the following:

1. Open the Control Panel.

2. If you are in Category view, click **Programs** and click **Programs and Features**. If you are in Icon view, double-click **Programs and Features**.
3. In the window shown in Figure 3.7, select a program and then click **Uninstall**. Some programs include the option to repair the program in addition to uninstalling it, but many simply offer the option to uninstall. To change the program, click **Change** or **Repair**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

If the program you want to uninstall isn't listed, it might not have been written for Windows 7. You should check the documentation for the software.

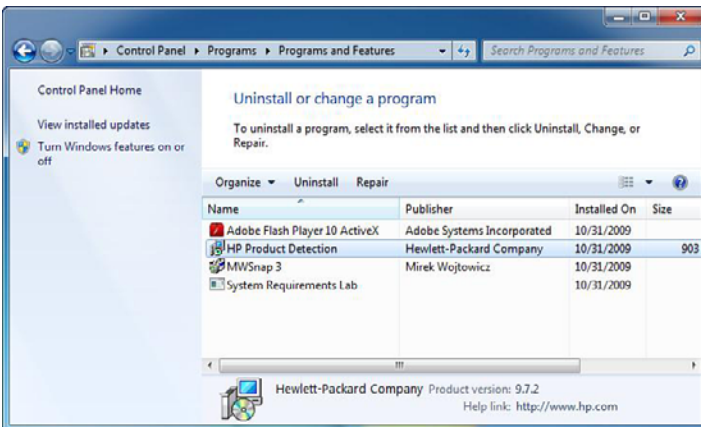


FIGURE 3.7 Uninstalling a program.

A default program is used to make a program the default for all file types and protocols it can open. For example, if you have more than one web browser installed on your computer, you can choose one of them to be the default program by using Set Default Programs. Another handy use is configuring a player (Windows Media Player or some other third-party player such as Real Player) to open all audio, music, and movie files.

If a program does not show up in the list or you want more control over which program opens up which files, you can make the program a default by using Set Association, also known as file association. For example, when you install Microsoft Word, Windows is configured so that anytime you double-click a file with a *.doc* or *.docx* filename extension, Microsoft Word automatically opens it.

To change the Set Association, do the following:

1. If you are in Category view, click **Programs** and click **Make a file type always open in a specific program**. If you are in Icon view, double-click **Default Programs** and click **Associate a file type or protocol with a program**. Figure 3.8 shows the resulting window.
2. Click the file type or protocol for which you want the program to act as the default.
3. Click **Change program**.
4. Click the program that you want to use as the default for the file type you selected, or click the arrow next to **Other programs** to show additional programs.
5. Click **OK**.

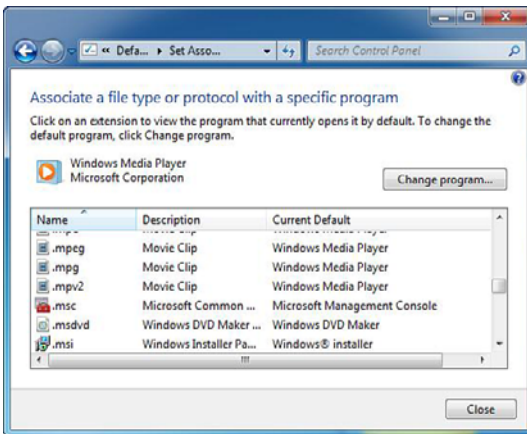


FIGURE 3.8 Changing the Set Association for a filename extension.

You can also right-click the file and select **Open With**. If the program you want to use to open the program does not appear in the Recommended Programs, you use the Browse button to browse to the program you do want to use. To change the filename association, be sure that the **Always use the selected programs to open this kind of file** checkbox is selected.

### ExamAlert

To configure which programs open up a filename as specified by their filename extension, you use either Set Default Programs or Set Association.

## Configuring Accessibility

Windows 7 includes accessibility technology, which enables computer users to adjust their computers to make them easier to see, hear, and interact with. The accessibility settings in Windows are particularly helpful to people with visual difficulties, hearing loss, pain in their hands or arms, or reasoning and cognitive issues.

Windows offers several programs and settings that can make the computer easier and more comfortable to use. You can add other assistive technology products to your computer if you need additional accessibility features.

The Ease of Access Center is a central location that you can use to set up the accessibility settings and programs available in Windows. As Figure 3.9 shows, in the Ease of Access Center, you find quick access for setting up the accessibility settings and programs included in Windows. You also find a link to a questionnaire that Windows can use to help suggest settings that you might find useful.

To open the Ease of Access Center, click the **Start** button, click **Control Panel**, click **Ease of Access**, and then click **Ease of Access Center**. Another way to access the Ease of Access Center is to press **Windows key + U**. You can open a mini Ease of Access Center by clicking the **Accessibility** icon, located on the bottom-left corner on the logon page.

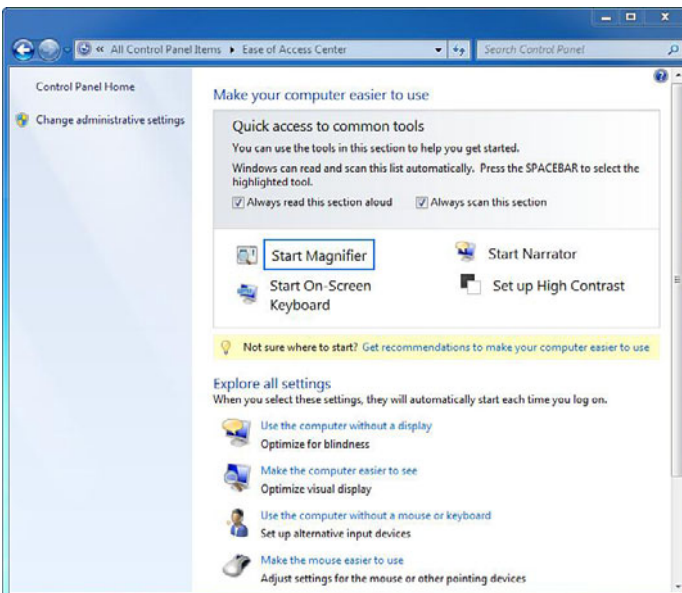


FIGURE 3.9 The Ease of Access Center.

The settings that can be adjusted are as follows:

- ▶ **Use the computer without a display:** Windows comes with a basic screen reader called Narrator that reads aloud text that appears on the screen. Windows also has settings for providing audio descriptions for videos and controlling how dialog boxes appear. For more information, search for **Use the computer without a display** using Windows Help and Support. Additionally, many other programs and hardware are compatible with Windows and available to help individuals who are blind, including screen readers, Braille output devices, and many other useful products.
- ▶ **Make the computer easier to see:** Several settings are available to help make the information on the screen easier to understand. For example, the screen can be magnified, screen colors can be adjusted to make the screen easier to see and read, and unnecessary animations and background images can be removed.
- ▶ **Use the computer without a mouse or keyboard:** Windows includes an on-screen keyboard that you can use to type. You can also use Speech Recognition to control your computer with voice commands as well as dictate text into programs.
- ▶ **Make the mouse pointer easier to use:** You can change the size and color of the mouse pointer, as well as use the keyboard to control the mouse.
- ▶ **Make the keyboard easier to use:** You can adjust the way Windows responds to mouse or keyboard input so that key combinations are easier to press, typing is easier, or inadvertent key presses are ignored.
- ▶ **Use text and visual alternatives for sounds:** Windows can replace two types of audio information with visual equivalents. You can replace system sounds with visual alerts and you can display text captions for spoken dialog in multimedia programs.
- ▶ **Make it easier to focus on reading and typing tasks:** There are a number of settings that can help make it easier to focus on reading and typing. You can have Narrator read information on the screen, adjust how the keyboard responds to certain keystrokes, and control whether certain visual elements are displayed.

**Note**

To find more information about assistive technology products, see the “Information for Assistive Technology Manufacturers” website at [www.microsoft.com/enable/at/atvinfo.aspx](http://www.microsoft.com/enable/at/atvinfo.aspx).

## Parental Controls

As a concerned parent, you want to protect your children. The Internet opens a new world of information gathering, communication, commerce, productivity, and entertainment; however, it also presents new risks for information disclosure, and easy access to inappropriate content in websites, messages, file downloads, games, and audio/video multimedia.

**ExamAlert**

Remember that Parental Controls are not available if the computer is part of a domain. They also apply only to standard user accounts.

Parental Controls are not available if your computer is connected to a domain. In addition, Parental Controls are only applied to standard user accounts, not administrative accounts. Of course, you need an Administrator user account to enable and configure Parental Controls.

To turn on Parental Controls for a standard user account:

1. Open Parental Controls by clicking the **Start** button, clicking **Control Panel**, and then, under User Accounts, clicking **Set up Parental Controls**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
2. Click the standard user account for which you want to set Parental Controls.
3. Under Parental Controls, click **On**.
4. After you’ve turned on Parental Controls for your child’s standard user account, you can adjust the individual settings that you want to control, as shown in Figure 3.10.

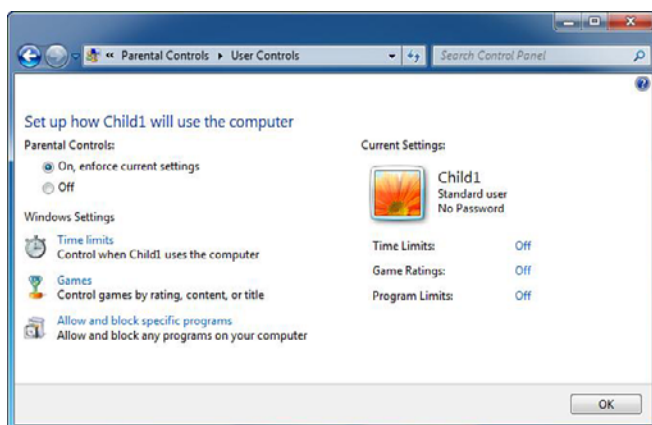


FIGURE 3.10 Parental Controls.

You can control the following areas:

- ▶ **Web restrictions:** You can restrict the websites that children can visit, make sure children only visit age-appropriate websites, indicate whether you want to allow file downloads, and set up which content you want the content filters to block and allow. You can also block or allow specific websites.
- ▶ **Time limits:** You can set time limits to control when children are allowed to log on to the computer. Time limits prevent children from logging on during the specified hours and, if they are already logged on, they are automatically logged off. You can set different logon hours for every day of the week.
- ▶ **Games:** You can control access to games, choose an age rating level, choose the types of content you want to block, and decide whether you want to allow or block unrated or specific games.
- ▶ **Allow or block specific programs:** You can prevent children from running programs that you don't want them to run.

After you've set up Parental Controls, you can set up activity reports to keep a record of your child's computer activity.



---

## Cram Quiz

1. You work as a desktop support technician at Acme.com. The new systems are using Windows 7 Home Basic edition. At Acme.com, you must ensure that users do not use instant messaging applications. What can you do?
  - A. Upgrade the systems to Windows 7 Professional. Then configure Parental Controls to disable the use of instant messaging applications.
  - B. Configure Parental Controls to only run allowed programs on each system.
  - C. Configure Parental Controls to enable the Windows 7 Web Filter.
  - D. Make sure that the users do not have administrative accounts on these local systems.
2. What can you use to determine which edition of Windows 7 you have?
  - A. Task Manager
  - B. Start Menu
  - C. Notification Area
  - D. System Properties
  - E. Welcome Center
3. You want to add Internet Information Services (IIS) to your Windows 7 installation. What should you do?
  - A. Use Default Program in the Control Panel
  - B. Use Set Association in the Control Panel
  - C. Use Windows Features in the Control Panel
  - D. Use Web Configuration in the Control Panel

## Cram Quiz Answers

- 1. B** is correct. You can use the Parental Controls to run only allowed programs that you specify. Answer A is incorrect because Windows 7 Home Basic edition already has Parental Control. Answer C is incorrect because Web filter does not stop messenger. Answer D is incorrect because you should not use administrative accounts to do daily tasks.
  - 2. D** is correct. To see the version and edition of Windows 7 that you are using, open the System Properties. The quickest way to get there is click the Start button, right-click Computer and select Properties. Answer E is incorrect because although the Welcome Center displayed the Windows Vista edition, this information is not displayed in the Welcome Center in Windows 7. Answers B, C, and D are incorrect because none of them show what version you are using.
  - 3. C** is correct. To add or remove Windows components, you use the Windows Features in the Control Panel. Answer A is incorrect because the Default Program makes a program the default for all file types and protocols it can open. Answer B is incorrect because Set Association is used to make a file or program always open a specific program. Answer D is incorrect because there is no Web Configuration in the Control Panel.
-

# Device Drivers

- ▶ **Configure devices.**
- ▶ **Configure system recovery options**

## CramSaver

1. What are the advantages of using signed drivers? (Choose all that apply.)
  - A.** You can verify where the driver came from.
  - B.** You can verify that the driver has not been tampered with.
  - C.** You can limit who has access to the driver.
  - D.** You can verify the driver has been thoroughly tested.
2. In Device Manager, how do you know if a device is disabled?
  - A.** There is a red X.
  - B.** There is an exclamation point.
  - C.** There is a down arrow.
  - D.** It is flashing.
3. You installed a new driver you got from the Internet for your sound card. Now the sound card does not work. What do you do to correct this problem?
  - A.** Enter Safe mode and remove the driver
  - B.** Rollback the driver
  - C.** Disable the device
  - D.** Uninstall the driver

## Answers

1. **A, B, and D** are correct. It is always recommended that you use signed drivers because you can verify where the driver came from, that the driver has not been tampered with, and that the driver has been thoroughly tested to be reliable. Answer C is incorrect because you cannot control who can access a specific driver.
2. **C** is correct. A down black arrow indicates a disabled device. A disabled device is a device that is physically present in the computer and is consuming resources, but does not have a driver loaded. Answer A is incorrect because a red X indicates a disabled device in Windows XP. Answer B is incorrect because problems with drivers are indicated by an exclamation point. Answer D is incorrect because if the device is having problems in the device manager, the device icon does not flash.

3. **B** is correct. When a new device driver does not function properly, you should roll it back so you can revert to the previous driver. Answers A and D are incorrect because uninstalling the driver means you still need to load the correct one. Answer C is incorrect because disabling the device causes the device not to function at all.

Device drivers are programs that control a device. They each act like a translator between the device and programs that use the device. Each device has its own set of specialized commands that only its driver knows. Most programs access devices by using generic commands, and the driver accepts the generic commands from the program and translates them into specialized commands for the device.

Device drivers are needed for a device to work. These drivers can be retrieved from the following sources:

- ▶ Bundled with Windows 7
- ▶ Supplied with a device
- ▶ Updated with Windows Update
- ▶ Updated from the manufacturer's Internet site

Sometimes, you might have to download an updated driver from Microsoft or the manufacturer's website to fix problems with device functionality caused by poorly written drivers or by changing technology.

The driver store is an extensive library of device drivers. On 32-bit computers, it is located in the `\Window\System32\DriverStore` folder. On a 64-bit computer, the 32-bit drivers are located in the `\Windows\SysWOW64\DriverStore` folder and the 64-bit drivers store is in the `\Windows\System32\DriverStore` folder. In the DriverStore folder, you find subfolders with located driver information, such as en-US for U.S. English, have thousands of different drivers. When you add a hardware device, Windows can check the Driver Store for the correct driver.

#### Note

Although the 64-bit version of Windows has a `Windows\SysWOW64\DriverStore` to store 32-bit drivers, you cannot use 32-bit drivers on a 64-bit version of Windows. Instead, you find Multilingual User Interface files that are used to display menus and dialog boxes in the designed language folders within the 32-bit DriverStore.

## Plug and Play Devices

Plug and play refers to the capability of a computer system to automatically configure expansion boards and other devices. You should be able to plug in a device and play with it, without worrying about setting DIP switches, jumpers, and other configuration elements. If you connect USB, IEEE 1394, and SCSI devices to a Windows 7 system, Windows 7 automatically detects these devices. When you connect a PCI or AGP plug-and-play expansion card and turn on the computer, Windows detects these devices. If Windows 7 does not have a driver available on the device after detection, Windows 7 prompts you to provide a media or path to the driver.

## Signed Drivers

To ensure reliable drivers, Microsoft implemented signed drivers starting with Windows 2000. A signed driver is a device driver that includes a digital signature, which is an electronic security mark that can indicate the publisher of the software and information that can show if a driver has been altered. When it is signed by Microsoft, the driver has been thoroughly tested to make sure that the driver will not cause problems with the system's reliability and not cause a security problem.

By default, if a driver is not signed, is signed by a publisher that cannot be properly identified, or has been altered since its release, Windows 7 notifies you. Of course, you should only install drivers that are properly signed.

### ExamAlert

A driver that lacks a valid digital signature, or that was altered after it was signed, can't be installed on x64-based versions of Windows Vista or 7.

Device drivers that are included on the Windows 7 installation DVD or downloaded from Microsoft's update website include a Microsoft digital signature (making it a signed driver). If you have problems installing a driver or a device is not working properly, you should check with Microsoft's update website and visit the device manufacturer's support website to obtain an up-to-date digitally signed driver for your device.

You can use the File Signature Verification program (Sigverif.exe) to check if unsigned device drivers are in the system area of a computer. You can obtain a basic list of signed and unsigned device drivers from a command prompt by running the **driverquery** command with the **/si** switch.

### ExamAlert

To verify that your drivers are properly signed, you should use the File Signature Verification program (Sigverif.exe).

## Devices and Printers Folder

When you want to see all the devices connected to your computer, use one of them, or troubleshoot one that isn't working properly, you can open the Devices and Printers folder found within the Control Panel.

The Devices and Printers folder gives you a quick view of devices connected to your computer, as Figure 3.11 shows.

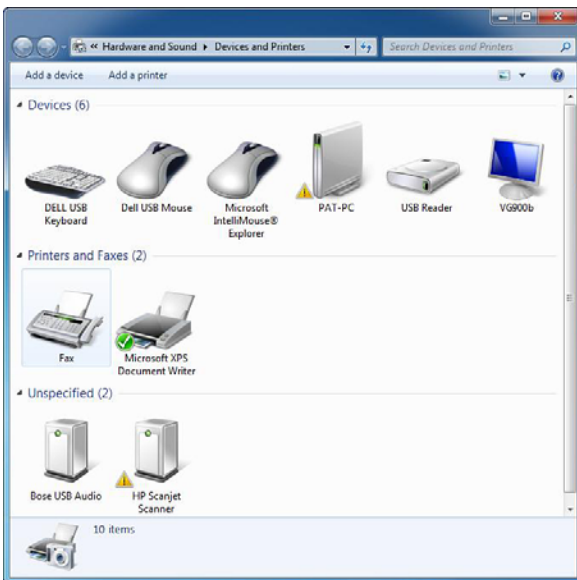


FIGURE 3.11 Devices and Printers folder.

These devices are typically external devices that you can connect to or disconnect from your computer through a port or network connection. Your computer is also displayed. The items displayed include

- ▶ Portable devices you carry with you and occasionally connect to your computer, such as mobile phones, portable music players, and digital cameras

- ▶ All devices you plug into a USB port on your computer, including external USB hard drives, flash drives, webcams, keyboards, and mice
- ▶ All printers connected to your computer, which include printers connected by USB cable, the network, or wirelessly
- ▶ Wireless devices connected to your computer, including Bluetooth devices and Wireless USB devices
- ▶ Your computer
- ▶ Compatible network devices connected to your computer, such as network-enabled scanners, media extenders, or Network Attached Storage devices (NAS devices)

The Devices and Printers folder does not display devices that are installed inside your computer case, such as internal hard drives, disc drives, sound cards, video cards (graphics cards), memory (RAM), processors, and other internal computer components. It does not display speakers connected to your computer with conventional speaker wires but might display USB and wireless speakers. The Devices and Printers folder also does not display legacy devices such as keyboards and mice connected through a PS/2 or serial port.

The Devices and Printers folder enables you to perform many tasks, which vary depending on the device. Here are the main tasks you can do:

- ▶ Add a new wireless or network device or printer to your computer
- ▶ View all the external devices and printers connected to your computer
- ▶ Check to see if a specific device is working properly
- ▶ View information about your devices, such as make, model, and manufacturer, including detailed information about the sync capabilities of a mobile phone or other mobile device

When you right-click a device icon in the Devices and Printers folder, you can select from a list of tasks that vary depending on the capabilities of the device. For example, you might be able to see what's printing on a network printer, view files stored on a USB flash drive, or open a program from the device manufacturer. For mobile devices that support the new Device Stage feature in Windows, you can also open advanced, device-specific features in Windows from the right-click menu, such as the ability to sync with a mobile phone or change ringtones.

If you have problems with devices, you can right-click a device or computer with the yellow warning icon and click **Troubleshooter** so that Windows can detect the problem. You would then follow the instructions on the screen.

## Device Manager

To find devices that are connected to your computer but aren't listed in the Devices and Printers folder, look in Device Manager. Device Manager lists all of the hardware installed inside your computer as well as devices connected externally. Device Manager is primarily for advanced computer users. When a device is added to the system, the device list in Device Manager is re-created.

To access the Device Manager, you must be logged on to the system as an administrator. To open Device Manager, click the **Start** button, click **Control Panel**, click **System and Security**, and then click **Device Manager** in the System section. Figure 3.12 shows the resulting window. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

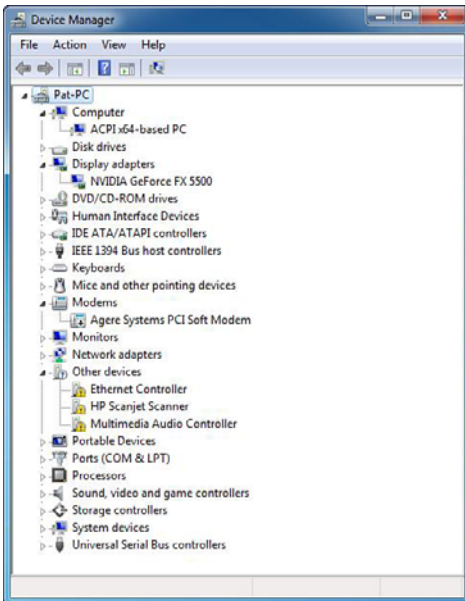


FIGURE 3.12 Device Manager.



If you locate and double-click a device, you can view the details of the driver in the General tab including the status of the device. If you select the Driver tab, as shown in Figure 3.13, you are able to do the following:

- ▶ **Driver File Details:** Shows the driver file and its location, the provider of the driver, the version of the file, and the digital signer of the file.
- ▶ **Uninstall a device:** The Device Manager tool can be used to uninstall the device driver and remove the driver software from the computer.
- ▶ **Enable or disable devices:** Instead of uninstalling the driver installer, you can use the Device Manager to disable the device. The hardware configuration is not changed.
- ▶ **Update device drivers:** If you have an updated driver for a device, you can use the Device Manager tool to apply the updated driver.
- ▶ **Roll back drivers:** If you experience system problems after you update a driver, you can roll back to the previous driver by using driver rollback. This feature enables you to reinstall the last device driver that was functioning before the installation of the current device driver. If there's no previous version of the driver installed for the selected device, the Roll Back Driver button is unavailable.

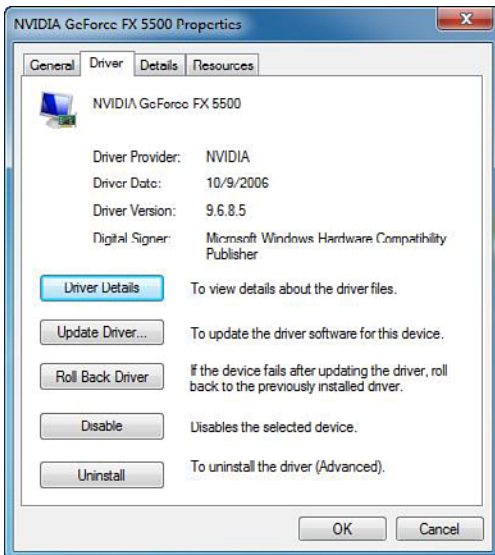


FIGURE 3.13 Device properties.

**ExamAlert**

If you load a driver and the device fails, it is recommended that you roll back the driver, assuming Windows is functioning well enough for you to access the properties of the device.

A down black arrow indicates a disabled device. A disabled device is a device that is physically present in the computer and is consuming resources but does not have a driver loaded. In Device Manager, a black exclamation point (!) on a yellow field indicates the device is in a problem state. You also need to look to see if any devices are listed under Unknown Device or have a generic name, such as Ethernet Adapter or PCI Simple Communications Controller, which indicates that the proper driver is not loaded.

**ExamAlert**

Be sure you know how to identify potential problems when using Device Manager, including devices with problems, disabled devices, and unknown devices.

## Adding a Device

Today, most modern devices are plug-and-play devices. Therefore, when you add or connect a new device, Windows 7 automatically recognizes the device and loads the appropriate driver. When a driver cannot be found, Windows might ask if you want to connect to the Internet in an attempt to find a driver or to specify the location of a driver such as on a CD. You can also open the **Control Panel**, click **Hardware and Sound**, and select **Add a device** under the Devices and Printers section. Windows then searches for any devices that are not currently recognized by Windows.

For more information about device management and installation for Windows 7, visit the following website:

[http://technet.microsoft.com/en-us/library/dd919230\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd919230(WS.10).aspx)

## Configuring Keyboard and Mouse

You can configure how the keyboard and mouse respond when using them. For example, if you open the Keyboard properties, you can configure how characters are repeated when you press a key and the rate that the cursor

blinks. The mouse Properties (see Figure 3.14) enables you to switch buttons, determine the speed of a double-click, determine what kind of pointer you want to use, and how fast the pointer moves when you move the mouse. In addition, depending on your type of mouse or pointing device, you might have additional options to configure, such as how many lines of a document or web page scroll when you move one notch on the wheel of the mouse or other pointing device.

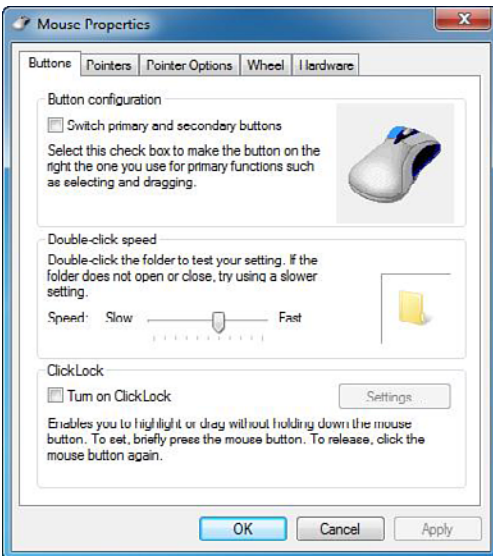


FIGURE 3.14 Mouse properties.

### Note

If you have a touch pad or track point, install the drivers that come with the touch pad. This gives you more control over your touch pad and automatically disables the track pad while you are typing so that you don't accidentally tap the touch pad, causing the cursor to jump to a different spot on the screen. When you stop typing, the track pad reactivates.

## Managing Sound

Today, most computers include a sound card, either one that is built into the motherboard or one that is added as an expansion card. You can use Sound in the Control Panel to configure the speakers, microphones, and sound theme.

As Figure 3.15 shows, a sound theme is a set of sounds applied to events in Windows and programs. For example, you can have one sound when you first log on to Windows and another sound when you shut down Windows. You can also modify the beep when an error occurs.

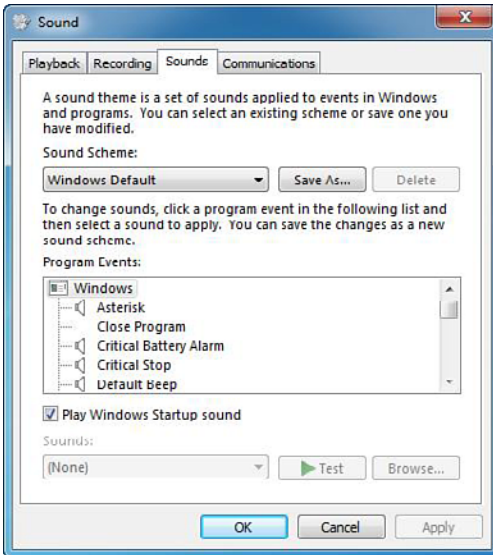


FIGURE 3.15 Sound properties.

When playing sound, there are several places that you might need to check when you want to control the volume. First, always check your speaker buttons and knobs. If you are using a laptop computer, you should look for keys on the keyboard to control volume. Second, check the program that you are using. For example, the Windows Media Player has a slider to control volume. Lastly, you should double-click the speaker icon in the notification area to open a slider to modify the volume. You can also click Mixer to give you more volume control such as speaker volume, application volume, and Windows Media Player volume, as shown in Figure 3.16. Of course, if you are getting no sound, make sure that the cables between the speakers (if they are external speakers) and sound card are plugged in properly.

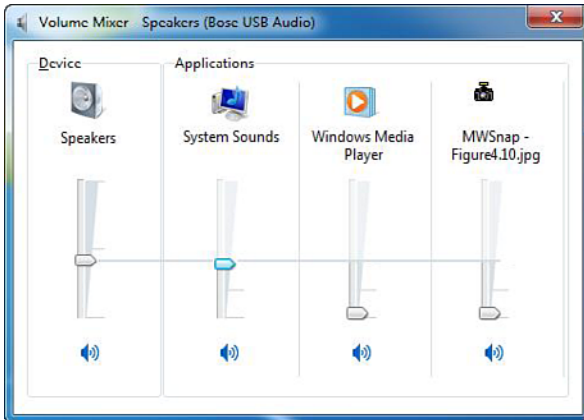


FIGURE 3.16 Volume Mixer.

---

## Cram Quiz

1. Different from Windows XP and Windows Vista, where do you manage your plug-in devices, including printers?
  - A. Device Manager
  - B. Administrative Tools
  - C. Devices and Printers Folder
  - D. Computer Management Console
2. Which driver cannot be installed on a 64-bit version of Windows 7? (Choose two answers.)
  - A. An unsigned device driver
  - B. A 32-bit driver
  - C. AGP drivers
  - D. Drivers that are not included on the Windows 7 Installation DVD
3. How do you have Windows 7 scan for new devices?
  - A. Run the `sigverif.exe` command
  - B. Run the `scandisk.exe` command
  - C. Click Hardware and Sound in the Control Panel and select Add a device under the Devices and Printers section
  - D. Run the `scanhw.exe` command

## Cram Quiz Answers

- 1. C** is correct. The Devices and Printers folder gives you a quick view of devices connected to your computer. These devices are typically external devices that you can connect or disconnect from your computer through a port or network connection. Answer A is incorrect because the Device Manager is a more advanced tool to manage all devices. The Devices and Printers folder enables you to control common settings for the plug-in devices. Answers B and D are incorrect because using the Computer Management Console, which is included in the Administrative Tools, enables you to access the Device Manager.
  - 2. A and B** are correct. A driver that lacks a valid digital signature, or that was altered after it was signed, cannot be installed on x64-based version of Windows Vista or 7. You also cannot load 32-bit drivers on a 64-bit system. Answer C is incorrect because AGP drivers can be loaded on a 64-bit version of Windows assuming they have been signed and are 64-bit drivers. Answer D is incorrect because you can also get device drivers from Microsoft and third-party websites. They just need to be signed by Microsoft.
  - 3. C** is correct. Often when you connect a device, it is automatically recognized and Windows 7 automatically tries to load the proper driver. If it doesn't, you need to select **Add a device** under the Devices and Printers section in the Control Panel so that Windows scans for hardware changes. Answer A is incorrect because `sigverif.exe` is used to verify the digital certificates for device drivers. Answer B is incorrect because `scandisk.exe` is the command to scan the disk in older versions of Windows. Answer D is incorrect because there is no `scanhw.exe` in Windows 7.
-

# Display Settings

## ► Configure devices

### CramSaver

1. If you don't see transparent windows on your Windows 7 desktop, what do you need to check?
  - A. Make sure Windows Aero is enabled
  - B. Make sure you have an Aero-compatible Super-VGA monitor
  - C. Make sure you are not using Windows 7 Home Premium, Enterprise, or Ultimate
  - D. Make sure you are not running with a Windows XP driver
2. You want to use two monitors so that you can double your workspace. What do you need to do?
  - A. Double the number of colors to display
  - B. Choose Screen Resolution and click Extend these displays
  - C. Choose Screen Resolution and click Copy this display
  - D. Choose Screen Resolution and click Duplicate these displays
3. What do you call a combination of pictures, colors, and sounds that specify the look and feel of your Windows graphical user interface?
  - A. A color display
  - B. Display Properties
  - C. Aero Properties
  - D. A theme

### Answers

1. **A** is correct. You need to make sure that Windows Aero is enabled. That means you have a display adapter that supports Windows Aero and you have to have a color depth of 32 bits per pixel, a refresh rate of 10 hertz or greater, select a Windows Aero theme, and have the Windows frame transparency on. Answer B is incorrect because there is no such thing as an Aero-compatible Super-VGA monitor. The compatibility is in the display adapter. Answer C is incorrect because Windows 7 Professional, Enterprise, Home Premium, and Ultimate support Windows Aero. Answer D is incorrect because you would not be able to load a Windows XP driver.

2. **B** is correct. When you connect another monitor to a desktop PC, the display is set to “extended” by default, and you should be able to drag a window from one screen to the other without changing any settings. Answer A is incorrect because the number of colors do not affect how many monitors you can use and how you can use them. Answer C is incorrect because there is no Copy this display option. Answer D is incorrect because you want to extend these displays, not duplicate these displays.
3. **D** is correct. A theme is a collection of visual elements and sounds for your computer desktop. A theme determines the look of the various visual elements of your desktop, such as windows, icons, fonts, and colors, and it can include sounds. Answer A is incorrect because there is no Color display in Windows 7. Answer B is incorrect because the display properties do not allow you to change your Windows GUI settings. Answer C is incorrect because there is no Aero Properties screen in Windows 7.

As a desktop technician, you are sometimes tasked with adjusting the look and feel of Windows, such as the background, the screen saver, and the display settings. You can find these settings by clicking the **Start** button, clicking **Control Panel**, clicking **Appearance and Personalization**, and clicking **Personalization** for the resulting screen in Figure 3.17. You can also right-click the desktop and select Personalize.

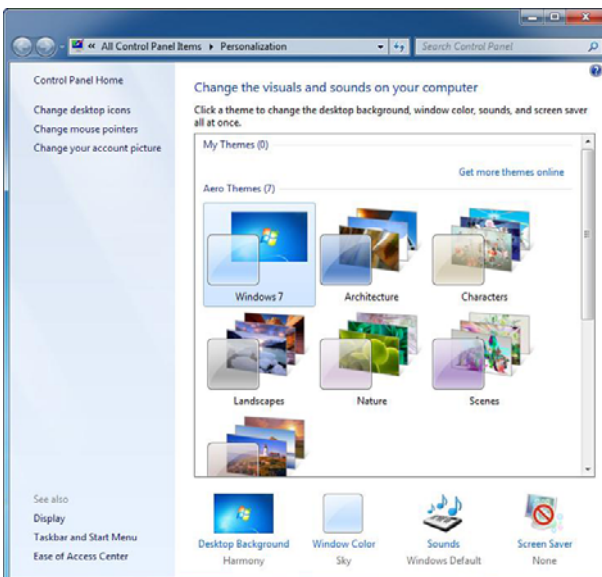


FIGURE 3.17 Personalizing appearance.



## Desktop Themes

A theme is a combination of pictures, colors, and sounds on your computer. It includes a desktop background, a screen saver, a window border color, and a sound scheme. Some themes might also include desktop icons and mouse pointers.

A theme determines the look of the various visual elements of your desktop, such as windows, icons, fonts, and colors, and it can include sounds. You can choose an Aero theme to personalize your computer, use the Windows 7 Basic theme if your computer is performing slowly, or a High Contrast theme to make the items on your screen easier to see.

To change the desktop theme in Windows 7:

1. Open Theme Settings by clicking the **Start** button, clicking **Control Panel**, clicking **Appearance and Personalization**, clicking **Personalization**, and then clicking **Change the Theme**.
2. In the Theme list, click an Aero Theme if you want to use Windows Aero. Other themes available are basic and high contrast themes.

At the bottom of the screen, you can also change the Desktop Background, the Windows color, sounds, and screen saver.

Windows Aero features windows that are truly translucent. This glass effect enables you to focus on the content of a window while providing better context for the surrounding elements on your desktop. For added personalization and to get exactly the look and feel you want, you can change the

- ▶ Color of your windows
- ▶ Saturation of the screen colors
- ▶ Level of transparency

To turn on window frame transparency, the color scheme must first be set to a Windows Aero theme. Then you must do the following:

1. Open Personalization by clicking the **Start** button, clicking **Control Panel**, clicking **Appearance and Personalization**, and then clicking **Personalization**.
2. Click **Window Color and Appearance**.
3. Select the **Enable transparency** checkbox.

You can also open Window Color and Appearance to change colors of individual components.

To configure Window color and appearance, do the following:

1. Click the **Start** button, click **Control Panel**, click **Appearance and Personalization**, click **Personalization**, and then click **Window Color and Appearance**.
2. You can then change the color of windows, Start menu, and taskbar, and you can enable or disable transparency, as demonstrated in Figure 3.18.

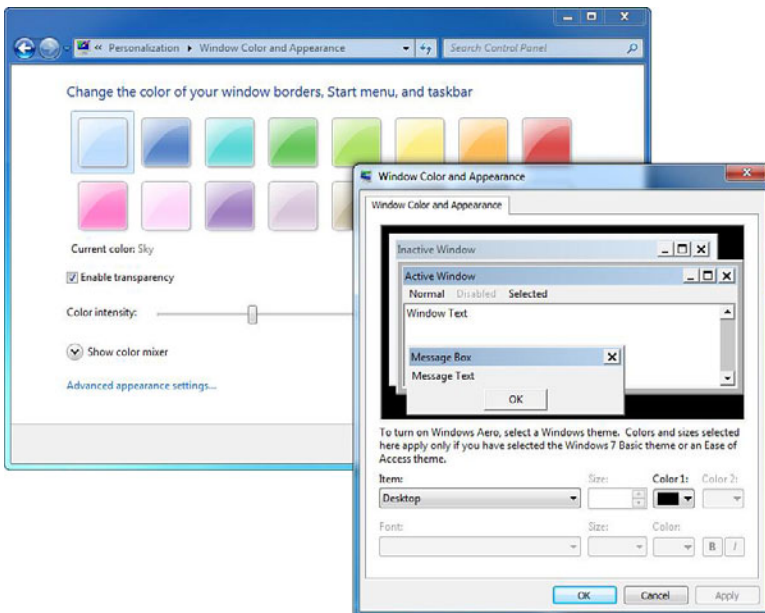


FIGURE 3.18 Configuring the Window Color and Appearance.

## Adjusting the Screen Settings

Screen resolution refers to the clarity of the text and images on your screen. At higher resolutions, items appear sharper because more pixels are used to form the images on the screen. Typically when you use a higher resolution, images appear smaller, so more items fit on the screen. At lower resolutions, fewer items fit on the screen, but they are larger and easier to see. At very low resolutions, however, images might have jagged edges.

To change the resolution, click **Display Settings** under **Personalization**.

1. If you are in Category view of Control Panel, click **Appearance and Personalization** and then click **Adjust screen resolution**. If you are in Icon view, you can double-click **Display** and select **Adjust resolution**. You can also right-click the desktop and choose **Screen resolution**.
2. In the resulting window shown in Figure 3.19, under Resolution, select the resolution and click **Apply** or **OK**.

**Note**

When you change the screen resolution, it affects all users who log on to the computer.

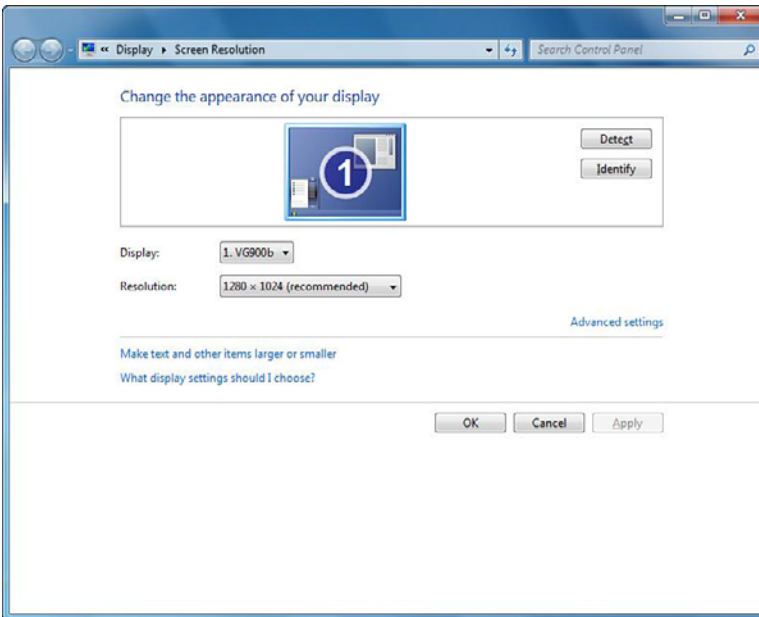


FIGURE 3.19 Changing resolution.

If you need to change the color depth (the number of bits that determine the number of possible colors on the screen) or the screen resolution (the frequency at which the screen is redrawn), under the Screen Resolution dialog box, click **Advanced settings** and select the **Monitor** tab, as shown in Figure 3.20. Then select the appropriate screen refresh rate or colors. For the most possible colors, select **True Color (32 bit)** and click **Apply** or **OK**.

### Note

Changes to the refresh rate or number of colors affect all users who log on to the computer.

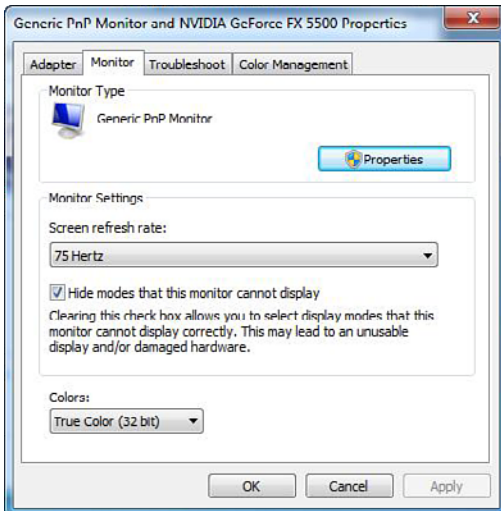


FIGURE 3.20 Changing colors.

If you sometimes have trouble seeing items on your screen, you can adjust the settings to make text and images on the screen appear larger, improve the contrast between items on the screen, and hear on-screen text read aloud. You can adjust these settings on the *Make the computer easier to see* page in the Ease of Access Center:

1. Open the **Make the computer easier to see** page by clicking the **Start** button, clicking **Control Panel**, clicking **Ease of Access**, clicking **Ease of Access Center**, and then clicking **Make the computer easier to see**.
2. Select the options that you want to use:
  - ▶ **Choose a High Contrast color scheme:** This option enables you to set a high-contrast color scheme that heightens the color contrast of some text and images on your computer screen, making those items more distinct and easier to identify.
  - ▶ **Turn on Narrator:** This option sets Narrator to run when you log on to your computer. Narrator reads aloud on-screen text and

describes some events (such as error messages appearing) that happen while you're using the computer.

- ▶ **Turn on Audio Description:** This option sets Audio Descriptions to run when you log on to your computer. Audio Descriptions describe what's happening in videos.
- ▶ **Turn on Magnifier:** This option sets Magnifier to run when you log on to your computer. Magnifier enlarges the part of the screen where the mouse is pointing and can be especially useful for viewing objects that are difficult to see.
- ▶ **Adjust the color and transparency of the window borders:** This option enables you to change the appearance of window borders to make them easier to see.
- ▶ **Make the focus rectangle thicker:** This option makes the rectangle around the currently selected item in dialog boxes thicker, which makes it easier to see.
- ▶ **Set the thickness of the blinking cursor:** This option enables you to make the blinking cursor in dialog boxes and programs thicker and easier to see.
- ▶ **Turn off all unnecessary animations:** This option turns off animation effects, such as fading effects, when windows and other elements are closed.
- ▶ **Remove background images:** This option turns off all unimportant, overlapped content and background images to help make the screen easier to see.

## Multiple Monitors

You can easily extend your Windows desktop across more than one monitor by plugging two or more monitors into a desktop computer or one or more monitors into a laptop. Most laptops allow you to connect one external monitor. A desktop that spans two or more monitors significantly increases your desktop area so that you can drag windows, program icons, and other items to any location on the extended desktop. To move a window from one display to another, click the title bar of the window and then drag the window to a new location.

By default, when you connect an external monitor to a laptop, the same image (mirror image) of your desktop appears on the external monitor. Before you can drag a window from your laptop screen to the external screen, you must extend your display by changing your display settings. By contrast, when you connect another monitor to a desktop PC, the display is set to “extended” by default, and you should be able to drag a window from one screen to the other without changing any settings.

To change your display settings to extended:

1. Right-click the desktop and choose **Screen Resolution**.
2. Click the drop-down list next to Multiple displays, click **Extend these displays**, and then click **OK**.

Your other options is to duplicate these displays, show desktop only on 1, and show desktop only on 2.

## Windows Aero

Windows Aero is an enhanced visual experience for Windows Vista and Windows 7. Different from older versions of Windows, Windows Aero supports transparent glass and other graphical enhancements that lead to a cosmetic pleasing display. In addition, you will notice smoother window control when opening, closing, moving, and resizing windows with increased stability.

Remember that the following editions of Windows 7 support Aero:

- ▶ Windows 7 Professional
- ▶ Windows 7 Enterprise
- ▶ Windows 7 Home Premium
- ▶ Windows 7 Ultimate

In addition to meeting the Windows edition prerequisite, the display adapter must support the following:

- ▶ DirectX 9, with Pixel Shader 2.0
- ▶ Windows 7 Display Driver Model (WDDM)

Finally, the system must have the following minimum graphics memory:

- ▶ **Graphics Memory:** Support single monitor resolution
- ▶ **64 MB:** Up to 1,310,720 pixels (equivalent to 1280×1024)
- ▶ **128 MB:** Up to 2,304,000 pixels (equivalent to 1920×1200)
- ▶ **256 MB:** Greater than 2,304,000 pixels

You must also configure the display system to the following:

- ▶ A color depth of 32 bits per pixel (bpp)
- ▶ A refresh rate that is higher than 10 hertz
- ▶ The theme is set to a Windows Aero theme
- ▶ Window frame transparency is on

### ExamAlert

Be sure to know which editions of Windows 7 include Windows Aero and the requirements for Windows 7 to enable Windows Aero. For Windows Aero to be automatically enabled in Windows 7, you must have a Windows Experience Index of 3.0 or higher.

If your system has a built-in graphics adapter based on the Unified Memory Architecture (UMA), you need 1 GB of dual-channel configured system memory and your system must have 512 MB of RAM available for general system activities after graphics processing.

If you receive a message that some visual elements, such as window frame transparency, have been turned off, if you receive a message that the color scheme has been changed to Windows Basic or Flip 3D does not function, one of the following might have happened:

- ▶ A program that you're running is incompatible with the Windows Aero color scheme. When you run a program that is incompatible with the Windows Aero color scheme, some visual elements are automatically turned off. When the program is no longer running, the visual elements that were turned off are turned on again automatically.
- ▶ Verify that your hardware configuration, screen resolution, theme, and color depths have not changed. Another cause could be because your computer does not have enough memory to run all of the programs that you have open and also run the Windows Aero color scheme.

To mitigate these issues, you should try closing some of the applications and retry the Flip 3D feature. If an application is incompatible with the Windows Aero color scheme, some of the visual elements are automatically disabled and then re-enabled after the incompatible application is closed.

---

## Cram Quiz

1. Which of the following does not support Windows Aero?
  - A. Windows 7 Professional
  - B. Windows 7 Enterprise
  - C. Windows 7 Home Basic
  - D. Windows 7 Home Premium
2. What do you call the option that specifies how many colors you can display at one time?
  - A. Color width
  - B. Color length
  - C. Color depth
  - D. Color resolution
3. Which of the following is not a requirement for Windows Aero?
  - A. Display adapter that supports DirectX 9.
  - B. Display adapter that supports the Windows Display Driver Model (WDDM).
  - C. A color depth of 32 bits per pixel.
  - D. Window frame transparency is off.

## Cram Quiz Answers

1. **C** is correct. Windows Aero is included with Windows 7 Professional, Enterprise, Home Premium, and Ultimate editions. It is not supported in Windows 7 Home Basic. Therefore, the other answers are incorrect.
  2. **C** is correct. The number of colors that can be displayed on a monitor is known as color depth. Answers A, B, and D are incorrect because there is no such thing as color width, length, or resolution. However, the resolution specifies how many pixels make up the screen.
  3. **D** is incorrect. Answers A, B, and C are incorrect because although you need to have a display adapter that supports DirectX 9 (Answer A), a display adapter that follows the WDDM (Answer B), and a color depth of 32 bits per pixel (Answer C), you also need to have the Windows frame transparency on. You also need to have a refresh rate of 10 hertz and you must be using a Windows Aero theme.
-



# Advanced Windows Configuration

- ▶ **Configure devices**
- ▶ **Supplemental Objectives: Manage and configure Windows**

## CramSaver

1. Which program would you use to perform advanced configuration including managing your users and groups, disks, Event Viewer, and shared folders and services?
  - A. Server Management console
  - B. Computer Management console
  - C. Task Scheduler
  - D. Local Security Policy
  
2. What do you call a program, routine, or process that performs a specific system function to support other programs?
  - A. A task
  - B. A service
  - C. An applet
  - D. A local policy

## Answers

1. **B** is correct. The Computer Management console enables you to manage local or remote computers by using a single, consolidated desktop tool. Using Computer Management, you can perform many tasks, such as monitoring system events, configuring hard disks, and managing system performance. Answer A is incorrect because the Server Management console is not available in Windows 7. Instead, it can be found on Windows Server 2008 computers. Answer C is incorrect because the Task Scheduler is used to schedule programs or other tasks to run automatically. Answer D is incorrect because the Local Security Policy enables you to view and edit group policy security settings.
  
2. **B** is correct. A service is a program, routine, or process that performs a specific system function to support other programs. To manage services, use the Services console located under Administrative Tools or the MMC with the Services snap-in. Answer A is incorrect because a task is a program or event that you can schedule with Task Manager. Answer C is incorrect because an applet is an icon found within the Control Panel. Answer D is incorrect because a local policy is used to configure the system settings, including how programs, network resources, and the operating system work for users.

## Microsoft Management Console

Microsoft Management Console (MMC) hosts and displays administrative tools created by Microsoft and other software providers. These tools are called snap-ins, and they are used for managing the hardware, software, and network components of Windows. Several of the tools in the Administrative Tools folder in Control Panel, such as Computer Management, are MMC snap-ins. The following section discusses the commonly used Administrative Tools found in Windows.

## Administrative Tools

Administrative Tools is a folder in Control Panel that contains tools for system administrators and advanced users. Many of the tools in this folder, such as Computer Management, are *Microsoft Management Console (MMC)* snap-ins that include their own help topics. To view specific help for an MMC tool, or to search for an MMC snap-in that you do not see in the following list, open the tool, click the **Help** menu, and then click **Help Topics**.

To access the Administrative Tools, open the Control Panel, open Administrative Tools by clicking **Start, Control Panel, System and Security** while in Category view, or double-click the Administrative Tools applet while in Icon view. You can also find it on the Start menu.

Some common administrative tools in this folder include the following:

- ▶ **Computer Management:** Manage local or remote computers by using a single, consolidated desktop tool. As shown in Figure 3.21, using Computer Management, you can perform many tasks, such as monitoring system events, configuring hard disks, and managing system performance.
- ▶ **Data Sources (ODBC):** Use Open Database Connectivity (ODBC) to move data from one type of database (a data source) to another.
- ▶ **Event Viewer:** View information about significant events, such as a program starting or stopping or a security error, that are recorded in event logs.
- ▶ **iSCSI Initiator:** Configure advanced connections between storage devices on a network.
- ▶ **Local Security Policy:** View and edit Group Policy security settings.
- ▶ **Memory Diagnostics Tool:** Check your computer's memory to see whether it is functioning properly.

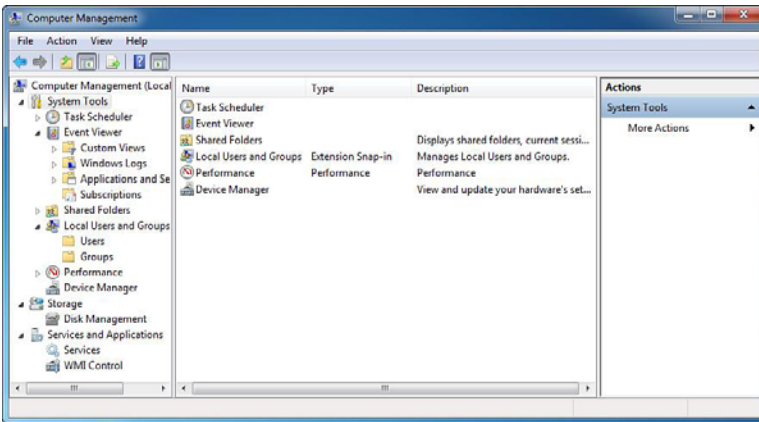


FIGURE 3.21 Computer Management.

- ▶ **Print Management:** Manage printers and print servers on a network and perform other administrative tasks.
- ▶ **Reliability and Performance Monitor:** View advanced system information about the central processing unit (CPU), memory, hard disk, and network performance.
- ▶ **Services:** Manage the different services that run in the background on your computer.
- ▶ **System Configuration:** Identify problems that might be preventing Windows from running correctly.
- ▶ **Task Scheduler:** Schedule programs or other tasks to run automatically.
- ▶ **Windows Firewall with Advanced Security:** Configure advanced firewall settings on both this computer and remote computers on your network.

### Note

You can access the Computer Management console by right-clicking **Computer** and selecting **Manage**.

## Services

A service is a program, routine, or process that performs a specific system function to support other programs. To manage the services, use the Services console located under Administrative Tools or the MMC with the Services

snap-in. The Services console is included in the Server Management console and the Computer Management console. To start, stop, pause, or resume services, right-click the service and click the desired option. On the left of the service name is a description.

To configure a service, right-click the service and click the **Properties** option. As shown in Figure 3.22, on the General tab, under the Startup type pull-down option, set the following:

- ▶ **Automatic:** Specifies that the service should start automatically when the system starts.
- ▶ **Automatic (Delayed Start):** Specifies that a service should be started approximately two minutes after the system has completed starting the operating system. It helps reduce the effect on the system's overall boot performance.
- ▶ **Manual:** Specifies that a user or a dependent service can start the service. Services with manual start-up do not start automatically when the system starts.
- ▶ **Disable:** Prevents the service from being started by the system, a user, or any dependent service.

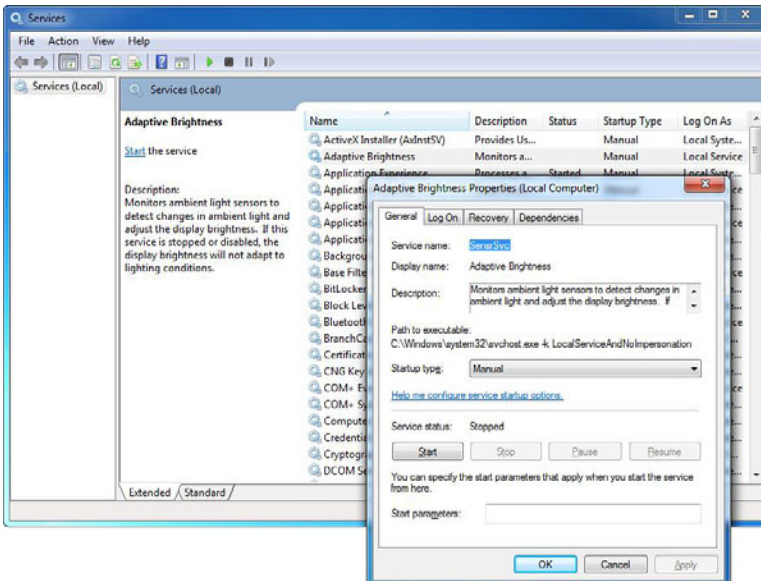


FIGURE 3.22 The Services Console.

## Local and Group Policies

Group Policy Objects (GPOs) are collections of user and computer configuration settings that specify how programs, network resources, and the operating system work for users and computers in an organization. Settings include the following:

- ▶ **System settings:** Application settings, desktop appearance, and behavior of system services.
- ▶ **Security settings:** Local computer, domain, and network security settings.
- ▶ **Software installation settings:** Management of software installation, updates, and removal.
- ▶ **Scripts settings:** Scripts for when a computer starts or shuts down and when a user logs on and off.
- ▶ **Folder redirection settings:** Storage for users' folders on the network.

Group policies can be set locally, on the workstation, or can be set at different levels (site, domain, or organizational unit) within Active Directory.

Microsoft's directory service is used for authentication and authorization. If you configure a group policy setting at the site, domain, or organization unit level and that setting contradicts a setting configured at the local policy, the group policy overrides the settings of the local policy.

You can open the Local Group Policy Editor by using the command line or by using the Microsoft Management Console (MMC). To open the Local Group Policy Editor from the command line click **Start**, type **gpedit.msc** in the Start Search box, and then press **Enter**.

To open the Local Group Policy Editor as an MMC snap-in:

1. Open MMC (click **Start**, click in the **Start Search** box, type **mmc**, and then press **Enter**).
2. On the File menu, click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins dialog box, click **Group Policy Object Editor** and then click **Add**.
4. With Local Computer already selected, click the **Finish** button.

Most times, you just need to access the security settings that you find in the local policy. You can do this by opening the Local Security Policy from Administrative Tools.

# The Registry

The registry is a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies. Components that use the registry include the Windows kernel, device drivers, setup programs, hardware profiles, and user profiles.

You shouldn't need to make manual changes to the registry because programs and applications typically make all the necessary changes automatically. An incorrect change to your computer's registry could render your computer inoperable. However, if a corrupt file appears in the registry, you might be required to make changes or to make a change that does not have a program to change. Typically if you are changing the registry, you are following instructions from a reliable source. The Registry Editor (Regedit.exe) is a tool used to manually view and change settings in the system registry, as shown in Figure 3.23.

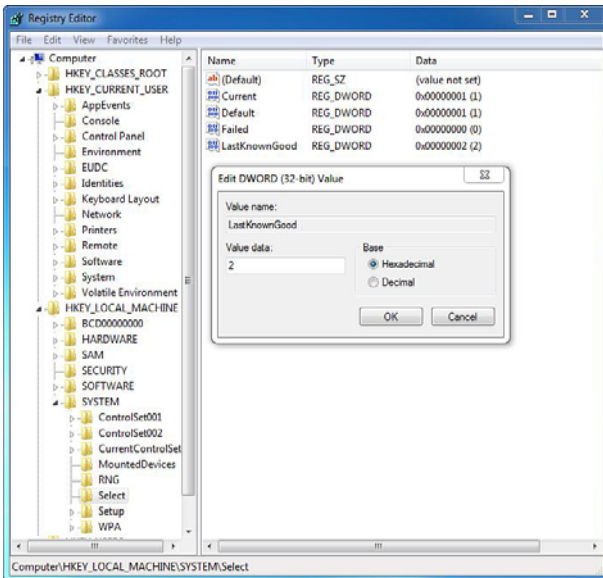


FIGURE 3.23 Using Regedit.exe to view the Registry.

The registry contains two basic elements: keys and values. *Registry Keys* are similar to folders; in addition to values, each key can contain subkeys, which may contain further subkeys, and so on. Keys are referenced with a syntax similar to Windows's path names, using backslashes to indicate levels of hierarchy. For example, HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows

refers to the subkey “Windows” of the subkey “Microsoft” of the subkey “Software” of the HKEY\_LOCAL\_MACHINE key. Windows 7 has five Root Keys:

- ▶ **HKEY\_CLASSES\_ROOT**: Stores information about registered applications, such as file associations.
- ▶ **HKEY\_CURRENT\_USER**: Stores settings that are specific to the currently logged-in user.
- ▶ **HKEY\_LOCAL\_MACHINE**: Stores settings that are specific to the local computer.
- ▶ **HKEY\_USERS**: Contains subkeys corresponding to the HKEY\_CURRENT\_USER keys for each user profile actively loaded on the machine, though user hives are usually only loaded for currently logged-in users.
- ▶ **HKEY\_CURRENT\_CONFIG**: Contains information gathered at run-time. Information stored in this key is not permanently stored on disk, but rather regenerated at boot time.

*Registry Values* are name/data pairs stored within keys. Values are referenced separately from keys. There are multiple types of values. Some of the common ones include the following:

- ▶ **REG\_SZ**: A string value
- ▶ **REG\_BINARY**: Binary data
- ▶ **REG\_DWORD**: A 32-bit unsigned integer (numbers between 0 and 4294967295 decimal)
- ▶ **REG\_MULTI\_SZ**: A multi-string value, which is an array of unique strings

Reg files (also known as Registration entries) are text files for storing portions of the registry. They have a .reg filename extension. If you double-click a reg file, it adds the Registry entries into the Registry. You can export any Registry subkey by right-clicking the subkey and choosing **Export**. You can back up the entire Registry to a reg file by right-clicking **Computer** at the top of Regedit and selecting **Export**.

---

## Cram Quiz

1. Where do you find the Windows Firewall with Advanced Security?
  - A. Administrative Tools
  - B. Registry Editor
  - C. Program Manager
  - D. File Manager
  
2. Which Registry Root Key stores settings that are specific to the local computer?
  - A. HKEY\_CLASSES\_ROOT
  - B. HKEY\_CURRENT\_USER
  - C. HKEY\_LOCAL\_MACHINE
  - D. HKEY\_USERS

## Cram Quiz Answers

1. **A** is correct. The Administrative Tools include the Computer Management Console, Event Viewer, Local Security Policy, Services console, Task Scheduler, and Windows Firewall with Advanced Security. Answer B is incorrect because the Registry Editor is used to configure the Registry, which is Windows's database of computer and user settings. Answers C and D are incorrect because there is no Program Manager or File Manager in Windows 7 to access the Windows Firewall.
  2. **C** is correct. The HKEY\_LOCAL\_MACHINE stores settings that are specific to the local computer. Answer A is incorrect because the HKEY\_CLASSES\_ROOT stores information about registered applications, such as file associated. Answer B is incorrect because the HKEY\_CURRENT\_USER stores settings that are specific to the currently logged-in user. Answer D is incorrect because the HKEY\_USERS contains subkeys corresponding to the HKEY\_CURRENT\_USER keys for each user profile actively loaded on the machine.
-



# Review Questions

1. Which of the following is not a good place to get device drivers? (Choose the best answer.)
  - A. Using a peer-to-peer search engine
  - B. Bundled with Windows 7
  - C. Supplied with a device
  - D. Updated with Windows Update
  - E. Updated from the manufacturer's website
2. In the Windows 7 Device Manager, how do you know if there is a problem with a driver? (Choose the best answer.)
  - A. The driver icon has a red X.
  - B. The driver icon has an exclamation point.
  - C. The driver icon has a down arrow.
  - D. The driver icon is flashing.
3. You work as a desktop support technician at Acme.com. You are tasked to install Windows 7 Enterprise Edition on computers that have been running Windows XP. You verified the video cards are WDDM-compatible. What else do you need to do to support Aero? (Each correct answer presents part of the solution. Choose three.)
  - A. Set the monitor settings to a refresh rate higher than 10
  - B. Press the Windows key + Tab
  - C. Set the resolution to 1280×1024 or higher
  - D. Set Color to 32 bit
  - E. Select a Windows Aero theme
  - F. Set the Color Scheme to Windows Aero
4. You are logged in with an administrator account on each Windows 7 Home Basic Edition. You have enabled Parental Controls, which restricts certain websites and only allows certain programs to run on the machine. You noticed that when you log in, you can access the restricted websites and run any software. What is the problem? (Choose the best answer.)
  - A. The system must be part of the domain, so the option is not available.
  - B. You just upgraded to the Windows 7 Ultimate edition.
  - C. Parental Controls only apply to standard users, and not administrative accounts.
  - D. Someone disabled the Parental Control on the system.

5. You work as a technician at Acme.com. You need to install a fingerprint reader. What should you do next? (Choose two answers.)
- A. Make sure that the application that uses the fingerprint reader is digitally signed
  - B. Make sure that the driver that you are installing is digitally signed
  - C. Connect the device before you load the driver
  - D. Load the driver before you connect the device
6. You were able to download a new printer driver from the Internet. How can you check the driver to make sure it is compatible with Windows 7?
- A. Right-click the driver and click Verify signing
  - B. Run the File Signature verification to verify that the new driver has a Microsoft digital signature
  - C. Install the driver and click the Verify Certificate button in the Device Manager
  - D. Install the driver and check the device logs in the Event Viewer
7. You have a report generator that uses .rep filename extensions. You want to modify Windows 7 so that when you double-click a file with the .rep filename extension, Internet Explorer opens with the report being displayed. What do you need to do?
- A. Open the Default Programs and select Set Association from the Control Panel
  - B. Right-click IExplore.exe and select Properties
  - C. Modify the filename association using registry
  - D. Modify the filename association using the local security policies
8. You have purchased some devices that have been sitting on the shelf at a store for several months and are about ready to be discontinued. You installed the drivers for those devices and now your system has some sporadic errors. What should you do?
- A. Look on the Windows CD for more up-to-date drivers
  - B. Check with the manufacturer's website and the Windows update website for more up-to-date drivers
  - C. Upgrade Windows 7 to the Ultimate edition so that it can make proper use of the drivers
  - D. Disable the prompting of unsigned driver warnings

9. You are a parent who wants your children to only run certain programs that you allow on the computer. What can you do?
- A. You should use Parental Controls on your computer to allow only certain programs.
  - B. You should use Ease of Access on your computer to allow only certain programs.
  - C. You should adjust your NTFS permissions so that they cannot install applications on your computer.
  - D. You should configure the firewall to block all ports not being used.
10. What console do you use to manage accessibility technology?
- A. Ease of Access Center
  - B. Accessibility
  - C. Disability
  - D. Computer Management

## Review Question Answers

1. Answer **A** is correct. Answers B, C, D, and E are recommended places to get drivers. Answer A is not a good place because you cannot verify where the driver came from or if it has been tampered with.
2. Answer **B** is correct. Problems with drivers are indicated by an exclamation point. Answer A is incorrect because a red X indicates a disabled device in Windows XP. Answer C is incorrect because a down arrow indicates a device is disabled. Answer D is incorrect because Device Manager does not flash.
3. Answers **A**, **D**, and **E** are correct. To enable Windows Aero, you must have set the monitor settings to a refresh rate higher than 10, set Color to 32 bit, and select a Windows Aero theme. Answer B is incorrect because the key combination does not enable or disable Windows Aero. Answer C is incorrect because the resolution is not a direct factor for Windows Aero. Different from Windows Vista, you do not have to select the Windows Aero color scheme (Answer F).
4. Answer **C** is correct. Parental Controls only affect standard users, not administrative users. Answer A is incorrect because Parental Controls would not have been enabled if it was part of a domain. Answer B is incorrect because you don't need to upgrade as Parental Controls are available in the Windows 7 Home Basic edition. Answer D requires an administrative account to disable Parental Controls. Therefore, it is unlikely this is correct.

5. Answers **B** and **C** are correct. To load drivers, you must have the device connected first. Then it is always recommended that you use signed drivers. Answer **A** is incorrect because applications do not have to be digitally signed. Answer **D** is incorrect because you have to have the device connected before you load the driver.
6. Answer **B** is correct. When you install new software, system files, and device drivers, unsigned or incompatible versions can cause system instability. Therefore, you should use the File Signature Verification to identify unsigned files on your computer, and you should not install drivers that do not have a proper driver signature. Answer **A** is incorrect because you cannot right-click the driver and click Verify signing. Answer **C** is incorrect because there is not a Verify Certificate button to click. Answer **D** is incorrect because there are no device logs in the Event Viewer and such information is not typically found in the Event Viewer.
7. Answer **A** is correct. When you want to change what program opens a particular type of data file, you should use the Control Panel's Default Program and select Set Association. Answer **B** is incorrect because there is no file associated or related option in the Internet Explorer properties. Answer **C** is incorrect because you could configure the filename association with the registry, but it is much more complicated than using the Control Panel. Answer **D** is incorrect because the local security policy cannot be used for filename association.
8. Answer **B** is correct because it is obvious that these drivers are not the newest. Therefore, you should check the Windows update website and manufacturer websites for newer drivers. Answer **A** is not the best answer because it might not have the newest drivers. Answer **C** is incorrect because the edition has no effect on how a driver is loaded. Answer **D** is incorrect because it is always recommended to load only signed drivers whenever possible.
9. Answer **A** is correct because if the computer is not part of the domain, you can use Parental Controls. Answer **B** is incorrect because you configure access to certain programs with Parental Controls and not Ease of Access. Answer **C** is incorrect because configuring NTFS is not the best way to configure accessibility options for children in this scenario. Answer **D** is incorrect because blocking ports is only partially effective and that would only block programs from communicating over the network.
10. Answer **A** is correct because the Ease of Access Center enables you to control the accessibility options. Answers **B** and **C** are incorrect because there are no such consoles with those names. Answer **D** is incorrect because the computer management is a powerful console but does not include accessibility options.

*This page intentionally left blank*

## CHAPTER 4

# Disk Management

**This chapter covers the following 70-680 Objectives:**

- ▶ Monitoring and Maintaining Systems That Run Windows 7:
  - ▶ Manage disks

Although most computers that run Windows 7 only have one hard drive, some have two or more hard drives. If your system only has one hard drive, it might be beneficial to take that one hard drive and divide it into multiple volumes so that you can run multiple operating systems or to isolate a data area. Besides using multiple drives and volumes, you also need to know how to optimize the drives. This includes configuring your drives with Redundant Array of Inexpensive Disks (RAID) to increase disk performance and reliability or using disk utilities to make the drives run efficiently. Therefore, as a desktop technician, you need to learn how to manage your disks in Windows 7.

# Disk Management Tools

## ► Manage disks

### CramSaver

1. What two commands or utilities are used to manage your disk volumes? (Choose two answers.)
  - A. Diskpart
  - B. Scandisk
  - C. Disk Management console
  - D. Shared Folders console
2. You installed Windows 7 on a new computer. You want to expand your C drive to a second hard drive. How should the disk be configured?
  - A. The disk needs to be a basic disk.
  - B. The disk needs to be a dynamic disk.
  - C. The disk needs to use MBR.
  - D. The disk needs to use GPT.

### Answers

1. **A and C** are correct. The two main programs or utilities to manage your disks are the Diskpart command and the Disk Management console. The Disk Management console can be found as part of the Computer Management console. Answer B is incorrect because Scandisk is a program found on older versions of Windows to check for errors. Answer D is incorrect because the Shared folders console, which is also part of the Computer Management console, is used to configure your shared folders.
2. **B** is correct. Dynamic disks do not have the same limitations of basic disks (Answer A). For example, you can extend a dynamic disk “on-the-fly” without requiring a reboot. In addition, dynamic disks can contain a virtually unlimited number of volumes, so you are not restricted to four volumes per disk as you are with basic disks. MBR (Answer C) and GPT (Answer D) are partitioning styles and have no bearing on the expanding or shrinking of a volume.

There are two main tools to manage your disks. The most common tool is the Disk Management console, which is part of the Computer Management console, as shown in Figure 4.1. With Disk Management, you can initialize disks, create volumes, and format volumes with the FAT, FAT32, or NTFS file systems.

Disk Management enables you to perform most disk-related tasks without restarting the system or interrupting users. Most configuration changes take effect immediately.

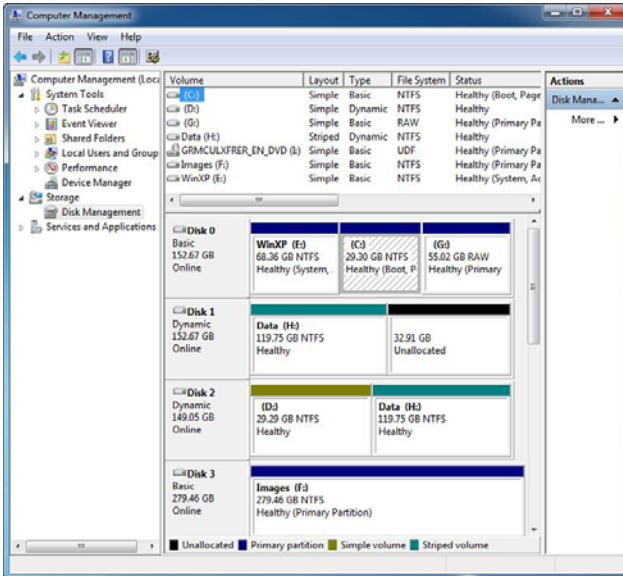


FIGURE 4.1 Disk Management console.

The other tool to manage your disks is Diskpart, which is a command-line hard disk partitioning utility included with Windows 2000, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, and Windows 7. It replaces `fdisk`, which was used in MS-DOS-based operating systems. You can use Diskpart to convert a basic disk to a dynamic disk. Diskpart is included as part of the Windows 7 operating system, and it can also be found as part of WinPE. Different from most commands executed at the command prompt, the `diskpart` command starts a command-based environment specifically used to manage your disks. It can also be used with scripts to automate its usage.

Before performing a specific operation using `diskpart`, you need to first change the focus or select the specific disk, partition, or volume using the `select` command. All commands except for `list`, `help`, `rem`, `exit`, or `help` require focus. To use the `select` command, you would do one of the following:

- ▶ **select**: To obtain a list of focus types, execute the `select` command with no parameters.
- ▶ **select disk[=n]**: Use the `select disk` command to set the focus to the disk that has the specified Windows disk number. If you do not specify a disk number, the command displays the current in-focus disk.



- ▶ **select partition [=n/1]:** Use the `select partition` command to set the focus to the specified partition. If you do not specify a partition, the current in-focus partition is displayed. On basic disks, you can specify the partition by either index, drive letter, or mount point. You can only specify the partition by index on dynamic disks.
- ▶ **select volume [=n/1]:** Use the `select volume` command to set the focus to the specified volume. If you do not specify a volume, the command displays the current in-focus volume. You can specify the volume by either index, drive letter, or mount point path. On a basic disk, if you select a volume, the corresponding partition is put in focus.

Use the `list` command to display a summary. To display more information, set the focus, and then use the `detail` command. Use the `detail disk` command to obtain the detailed information about the current in-focus disk. Of course, with each of these, you use either disk, partition, or volume (see Figure 4.2). After you have selected your drive, partition, or volume, you then use create partition, delete partition, create volume, or delete volume. Lastly, you use the `exit` command to exit diskpart.

```

Administrator: C:\Windows\system32\cmd.exe - diskpart
C:\Users\patrickreg>diskpart
Microsoft DiskPart version 6.1.7600
Copyright (c) 1998-2008 Microsoft Corporation.
On computer: BEST7LPR

DISKPART> list disk

Disk ### Status      Size  Free  Dyn  Gpt
-----
Disk 0   Online         298 GB  1024 KB

DISKPART> select disk=0
Disk 0 is now the selected disk.

DISKPART> list partition

Partition ### Type          Size  Offset
-----
Partition 1  Primary     1200 MB  1024 KB
Partition 2  Primary     144 GB  1201 MB
Partition 0  Extended   142 GB  145 GB
Partition 4  Logical     142 GB  145 GB
Partition 3  Primary     10 GB   287 GB

DISKPART> select partition 2
Partition 2 is now the selected partition.

DISKPART> detail volume

Disk ### Status      Size  Free  Dyn  Gpt
-----
* Disk 0   Online         298 GB  1024 KB

Read-only          : No
Hidden             : No
No Default Drive Letter : No
Shadow Copy        : No
Offline            : No
BitLocker Encrypted : No
Installable        : Yes

Volume Capacity   : 144 GB
Volume Free Space  : 83 GB

DISKPART>

```

FIGURE 4.2 Using Diskpart to select and list a volume.

For more information about the `diskpart` utility, visit the following website:  
<http://support.microsoft.com/kb/300415>

### Note

To create a fourth primary partition on a basic disk, you must use the `diskpart` utility. It cannot be done with the Disk Management console.

## Disk Partitioning

When you prepare any drive or volume to be used by Windows 7, you must first partition the disk and then format the disk. Partitioning is defining and dividing the physical or virtual disk into logical volumes called *partitions*. Each partition functions as if it were a separate disk drive.

Windows 7 supports two types of disk partitioning styles: Master Boot Record (MBR) and GUID partition table (GPT). Therefore, when you install a new drive, you need to choose which type of partition style you want to use.

MBR disks have been used as *standard equipment* on IBM-compatible personal computers since the days of MS-DOS. MBR disks support volume sizes up to two terabytes (TB) and allow up to four primary partitions per disk. Alternatively, MBR disks support three primary partitions, one extended partition, and an unlimited number of logical drive letters created within the extended partition.

Windows 7 includes support for GPT disks in cluster storage. GPT disks were introduced with computers equipped with Intel Itanium-based processors and the Extensible Firmware Interface (EFI) instead of using a Basic Input/Output System (BIOS) as the interface between the computer's hardware devices, its firmware, and the operating system. GPT provides a more flexible mechanism for partitioning disks than the older MBR partitioning scheme that has been common to PCs. GPT disks support volume sizes up to 18 Exabytes (EB) and can store up to 128 partitions on each disk. Eighteen Exabytes are roughly equivalent to 18 billion Gigabytes. Critical system files are stored on GPT partitions, and GPT disks store a duplicate set of partition tables to ensure that partitioning information is retained. Although GPT has been around a while, no x86 version of Windows prior to Windows Vista supported it. Windows XP Professional x64 does support it.

**ExamAlert**

If you have disks that are greater than 2 TB, you must use GPT.

The *active partition* is the partition or volume that is marked as the partition to boot from. Therefore, it is expected to have the necessary boot files. The active partition or volume that contains the boot file is known as the *system partition/volume*. The partition or volume that contains the Windows operating system (such as the Windows folder) is called the *boot partition*. If a system has only one partition with the initial boot files and the Windows folder, then the partition is both the system partition and the boot partition.

**ExamAlert**

As strange as it sounds, the system volume contains the Windows boot files and the boot volumes contains the Windows operating system files.

The `%systemroot%` or *systemroot* indicates the folder into which Windows 7 is installed, which is located on the boot partition. By default, the Windows 7 system root directory is `C:\Windows`.

## Disk Storage Management

Windows 7 supports two types of hard disk storage: basic and dynamic. All disks begin as basic disks until an administrator converts them to dynamic status, one physical disk at a time. The biggest advantage that dynamic disks offer when compared to basic disks is that you can create software-based fault-tolerant volumes via the operating system from the volumes stored on dynamic disks using mirrored volumes (RAID 1). Of course, you can always implement a hardware RAID solution using a RAID controller, which supports striping with parity (RAID 5).

**Note**

RAID is short for redundant array of inexpensive disks (or redundant array of independent disks). RAID is technology that provides high levels of storage reliability from low-cost and less reliable disk drives.

## Basic Disks

A basic disk under Windows 7 is essentially the same as the disk configuration under earlier versions of Windows—it is a physical disk with primary and extended partitions. You can create up to three primary partitions and one extended partition on a basic disk or four primary partitions. Primary partitions are partitions from which you can boot an operating system. You can divide an extended partition into numerous logical drives. Basic disks store their configuration information in the *partition table*, which is stored on the first sector of each hard disk. The configuration of a basic disk consists of the partition information on the disk.

## Dynamic Disks

A Windows 7 dynamic disk is a physical disk configuration that does not use partitions or logical drives, and the MBR is not used. Instead, the basic partition table is modified and any partition table entries from the MBR are added as part of the Logical Disk Manager (LDM) database that stores dynamic disk information at the end of each dynamic disk. You can divide dynamic disks into as many as 2,000 separate volumes, but you should limit the number of volumes to 32 for each dynamic disk to avoid slow boot time performance. Of course, this type of configuration is most likely found on servers.

Dynamic disks do not have the same limitations as basic disks. For example, you can extend a dynamic disk “on-the-fly” without requiring a reboot. Dynamic disks are associated with disk groups, which are disks that are managed as a collection. This managed collection of disks helps organize dynamic disks. All dynamic disks in a computer are members of the same disk group. Each disk in a disk group stores replicas of the same configuration data. This configuration data is stored in the 1 MB LDM region at the end of each dynamic disk.

Dynamic disks support four types of volumes: simple, spanned, mirrored, and striped. Although the option for RAID-5 is listed with dynamic disks, the option is not available for desktop operating systems including Windows 7. Therefore, the option is grayed out. Dynamic disks can contain a virtually unlimited number of volumes, so you are not restricted to four volumes per disk as you are with basic disks.

## Managing Basic Disks and Dynamic Disks

When you install Windows 7, the system automatically configures the existing hard disks as basic NTFS disks, unless they have been configured as dynamic from a previous installation. Windows 7 does not support dynamic disks on

mobile PCs (laptops or notebooks). If you're using an older desktop machine that is not Advanced Configuration and Power Interface (ACPI) compliant, the Convert to Dynamic Disk option is not available. Dynamic disks have some additional limitations. You can install Windows 7 on a dynamic volume that you converted from a basic disk, but you cannot extend either the system or the boot volume on a dynamic disk. Any troubleshooting tools that cannot read the dynamic disk management database work only on basic disks.

### ExamAlert

Dynamic disks are supported only on computers that use the Small Computer System Interface (SCSI), Fibre Channel, Serial Storage Architecture (SSA), or Integrated Drive Electronics (IDE). Portable computers, removable disks, and disks connected via Universal Serial Bus (USB) or FireWire (IEEE 1394) interfaces are not supported for dynamic storage. Dynamic disks are also not supported on hard drives with a sector size of less than 512 bytes.

To make a partition active so that it can boot the operating system boot files, you just need to right-click the volume in the Disk Management add-in and select the Mark Partition as Active. If the boot files do not exist, you get a message such as “Non-system disk” or a similar message.

## Converting Basic Disks to Dynamic Disks

From the graphical user interface (GUI), you use the Windows 7 Disk Management console (an MMC snap-in) to upgrade a basic disk to a dynamic disk. The Disk Management snap-in is located in the Computer Management console and the Server Management console. You must be a member of the local Administrators group or the backup operators group, or else the proper authority must be delegated to you if you are working within an Active Directory environment to make any changes to the computer's disk-management configuration.

For the conversion to succeed, any disks to be converted must contain at least 1 MB of unallocated space. Disk Management automatically reserves this space when creating partitions or volumes on a disk, but disks with partitions or volumes created by other operating systems might not have this space available. (This space can exist even if it is not visible in Disk Management.) Windows 7 requires this minimal amount of disk space to store the dynamic database, which the operating system that created it maintains. In addition, you cannot convert drives that use an allocation unit size greater than 512

bytes. Before you convert any disks, close any programs that are running on those disks.

If your computer can multiboot between different versions of Windows, you should not convert to dynamic disk because you will not be able to start installed operating systems from any volume on the disk, except the current boot volume. In addition, other operating systems might not be able to read dynamic disks.

To convert a basic disk to a dynamic disk from the Disk Management console, perform the following steps:

1. Open the Disk Management console.
2. Right-click the basic disk that you want to convert to a dynamic disk and then click **Convert to Dynamic Disk**.

When you upgrade an empty basic disk to a dynamic disk, you do not need to reboot. However, if you convert a basic disk that already has partitions on it, or if the basic disk contains the system or boot partitions, you must restart your computer for the change to take effect.

To convert a basic disk to a dynamic disk from the Windows 7 command line, perform these steps:

1. Open a command prompt window, type **diskpart**, and press **Enter**.
2. Type **commands** or **help** to view a list of available commands.
3. Type **select disk 0** to select the first hard disk (**select disk 1** to select the second hard disk, and so on) and press **Enter**.
4. Type **convert dynamic** and press **Enter**.
5. Type **exit** to quit the **diskpart.exe** tool and then restart the computer to have the new configuration take effect.

When you convert a basic disk to a dynamic disk, any existing partitions on the basic disk become simple volumes on the dynamic disk. Any existing mirror sets, stripe sets, stripe sets with parity, or volume sets become mirrored volumes, striped volumes, dynamic RAID-5 volumes, or spanned volumes, respectively. After you convert a basic disk to a dynamic disk, you cannot change the volumes back to partitions.

Because the conversion process from basic to dynamic is per physical disk, a disk has all dynamic volumes or all basic partitions; you won't see both on the same physical disk. Remember, you do not need to restart your computer

when you upgrade from an empty basic to a dynamic disk from the Disk Management console. However, you do have to restart your computer if you use the `diskpart.exe` command-line tool for the conversion; if you convert a disk containing the system volume, boot volume, or a volume with an active paging file; or if the disk contains any existing volumes or partitions.

### ExamAlert

When you upgrade or convert a basic disk to a dynamic disk, at least 1 MB of free space must be available for the dynamic disk database. Under normal circumstances, this requirement should not be a problem.

## Converting Dynamic Disks Back to Basic Disks

You must remove all volumes (and therefore all data) from a dynamic disk before you can change it back to a basic disk. After you convert a dynamic disk back to a basic disk, you can only create partitions and logical drives on that disk. After being converted from a basic disk, a dynamic disk can no longer contain partitions or logical drives, nor can any operating systems other than newer versions of Windows. To revert a dynamic disk to a basic disk, perform the following steps:

1. Back up the data on the dynamic disk.
2. Open Disk Management.
3. Delete all the volumes on the disk.
4. Right-click the dynamic disk that you want to change back to a basic disk and then click **Convert to Basic Disk**.
5. Restore the data to the newly converted basic disk.

The disk structure does not describe how a hard drive or floppy disk physically works, but how it stores files on the disk. In other words, it describes the formatting of the disk (file system, partitions, the root directory, and the directories). A file system is the overall structure in which files are named, stored, and organized. File systems used in Windows 7 include FAT, FAT32, and NTFS. Although FAT and FAT32 were primarily used in older operating systems, NTFS is the preferred file system.

**ExamAlert**

Converting to a dynamic disk is a one-way process. Yes, you can convert a dynamic disk back to a basic disk, but you lose all your data. Obviously, this loss is a major consideration! If you find yourself needing to do it, first back up your data and then you can delete all the volumes on the disk, convert the disk to basic, and restore your data.

## File Systems

An older file system used by DOS was the file allocation table (FAT). FAT is a simple file system that uses minimum memory. Although it is based on file names of 11 characters, which include the 8 characters for the file name and 3 characters for the file extension, it has been expanded to support long file-names. Early DOS used FAT12, which used a 12-bit number for each cluster, but was later expanded to FAT16, which recognized volumes up to 2 GB.

FAT32, which was introduced in the second major release of Windows 95, was an enhancement to the FAT file system. It uses 32-bit FAT entries, which supports hard drives up to 2 TB, although Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008 (including R2) support volumes up to 32 GB. FAT32 does not have the security that NTFS provides, so if you have a FAT32 partition or volume on your computer, any user who has access to your computer can read any file on it. Today, the only time you use FAT32 is in the event that you have a computer that can boot to multiple operating systems, and one of the other operating systems (such as Windows 95 or 98) cannot read and write to NTFS. Systems that can load more than one operating system are known as having a *multi-boot configuration*.

NTFS is the preferred file system for Windows XP and later versions. It has many benefits over the FAT and FAT32 file systems, including

- ▶ Improved support for much larger hard disks
- ▶ Some automatic recovery of disk-related errors because it is a journaling file system that keeps track of its transactions to make sure that that entire transaction is completed before being recognized
- ▶ Better security because you can use permissions and encryption to restrict access to specific files to approved users
- ▶ Disk compression
- ▶ Disk quotas



Another file system used in Windows 7 is Extended File Allocation Table (exFAT), sometimes referred to as FAT64. ExFAT is a new file system that is better adapted to the growing needs of mobile personal storage such as USB flash drives that require minimum overhead. Although exFAT can theoretically handle up to 64 ZB (a Zettabyte (ZB) is equal to 1 billion Terabytes), 512 TB is the recommended maximum. It can also handle files that are larger than 4 GB. Unfortunately, exFAT does not support the encryption and permission features found in NTFS.

---

## Cram Quiz

1. You have a new hard drive that has 4 TB. What type of partitioning style do you need to use?
  - A. GPT
  - B. MBR
  - C. Basic
  - D. Dynamic
2. How do you convert a dynamic disk to basic disk?
  - A. Right-click the dynamic disk and select **Convert to Basic Disk** in the Disk Management console.
  - B. Right-click the disk in Windows Explorer and select Format. In the Format dialog box, select **Basic format**.
  - C. Specify the convert command using **diskpart**.
  - D. Back up all data on the dynamic disk. Delete the disk. Re-create the disk as a Basic Disk. Restore the data.

## Cram Quiz Answers

1. **A** is correct. Partitioning is defining and dividing the physical or virtual disk into logical volumes called partitions. Each partition functions as if it were a separate disk drive. Windows 7 supports two types of disk partitioning styles: Master Boot Record (MBR) and GUID partition table (GPT). If you have disks that are greater than 2 TB, you must use GPT because MBR (Answer B) does not support disks larger than 2 TB. Answers C and D are incorrect because Basic and Dynamic disks describe the type of hard disk storage.
  2. **D** is correct. Converting a basic disk to a dynamic disk is a one-way process. Therefore, the only way to convert a dynamic disk back to a basic disk is to delete the old disk and re-create it. Because that loses all data, you need to back up first and restore after you are done; therefore, the other answers are incorrect.
-

# Working with Volumes

► Manage disks

## CramSaver

1. You have a new Windows 7 computer with multiple hard drives. You want to implement RAID1 on the computer. What do you need to do first?
  - A. Enable write caching on the first disk
  - B. Enable write caching on the second disk
  - C. Convert the basic disk to dynamic disks
  - D. Convert the dynamic disk to basic disks
2. You have a computer running Windows 7. Your system has a large hard drive with one volume that holds the Windows 7 volume. Out of 500 GB, you realize that you are only using approximately 100 GB. You decide you want to create a new volume on disk 0. What should you do?
  - A. Compress volume C
  - B. Create a virtual hard disk (VHD)
  - C. Shrink volume C
  - D. Configure a disk quota for volume C
3. What is the maximum number of volumes you can add to a striped volume?
  - A. 2
  - B. 4
  - C. 8
  - D. 16
  - E. 32

## Answers

1. **C** is correct. RAID1 (disk mirroring) needs two disks to implement. Before you can enable RAID1 using Windows 7, you need to convert basic disks to dynamic disks, which converts the partitions into volumes. Answers A and B are incorrect because write caching only improves disk performance and does not help implement RAID1. Answer D is incorrect because to implement RAID1 using Windows 7, you must use dynamic disks.

2. **C** is correct. To make room for the new volume, you can shrink the system drive assuming the disk drive is set to dynamic. Answer A is incorrect because compressing volume C only gives you more disk space on the C drive but does not shrink the volume itself. Answer B is incorrect because a virtual hard disk can be attached to a system, but it does not add a volume to the 500 GB drive. Answer D is incorrect because disk quotas help you manage the disk to make sure users do not use too much disk space.
3. **E** is correct. A striped volume can contain up to 32 volumes. Therefore, the other answers are incorrect.

You can create primary partitions, extended partitions, and logical drives only on basic disks. Partitions and logical drives can reside only on basic disks. You can create up to four primary partitions on a basic disk or up to three primary partitions and one extended partition. You can use the free space in an extended partition to create multiple logical drives. You must be a member of the local Administrators group or the backup operators group, or else the proper authority must be delegated to you (if you are working within an Active Directory environment) to create, modify, or delete basic volumes.

You must first create an extended partition before you can create a new logical drive, if no extended partition exists already. If you choose to delete a partition, all data on the deleted partition or logical drive is lost. You cannot recover deleted partitions or logical drives. You cannot delete the system partition, boot partition, or any partition that contains an active paging file. The operating system uses one or more paging files on disk as virtual memory that can be swapped into and out of the computer's physical random access memory (RAM) as the system's load and volume of data dictate.

### ExamAlert

Windows 7 requires that you delete all logical drives and any other partitions that have not been assigned a drive letter within an extended partition before you delete the extended partition itself.

With dynamic disks, you are no longer limited to four volumes per disk (as you are with basic disks). As mentioned before, Windows 7 supports simple, spanned, mirrored, and striped volumes. You must be a member of the local Administrators group or the backup operators group.

## Simple Volumes

A simple volume consists of disk space on a single physical disk. It can consist of a single area on a disk or multiple areas on the same disk that are linked together. To create a simple volume using the Disk Management console, perform the following steps:

1. Open Disk Management.
2. Right-click the unallocated space on the dynamic disk where you want to create the simple volume and then click **New Simple Volume**.
3. When the Welcome to the New Simple Volume Wizard appears, click **Next**.
4. Specify the size of the volume and click **Next**.
5. When it asks you to assign a drive letter or path as shown in Figure 4.3, select a drive letter and click **Next**.
6. Choose a file system (NTFS is recommended). You should also specify a name for the volume so that it can be easier to identify. You can then perform a quick format (or a long format if you don't select quick format) and enable file and folder compression if desired.
7. When the summary appears, click the **Finish** button.

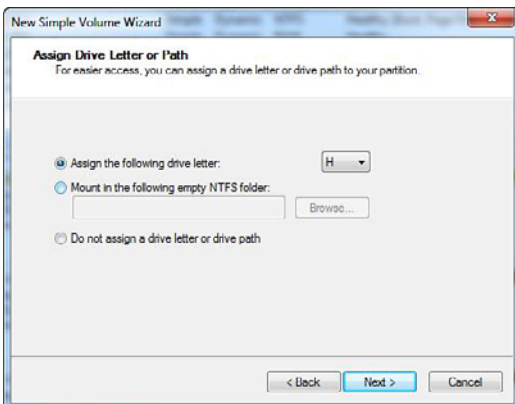


FIGURE 4.3 Assigning a drive letter or path to a simple volume.

To create a partition primary of length size and a starting address offset on the current drive using the `diskpart` command prompt, you use the following command:

```
create partition primary size=xxx
```

After the partition is created, the new extended partition gains the focus.

To create a simple volume of length size at the diskpart command prompt, you use the following command:

```
create volume simple size=xxx disk=n
```

If you do not specify a size, the new volume can take up the remaining contiguous free space on the disk. If you do not specify a disk, the current in-focus disk is used. After the volume is created, the disk focus is given to the targeted disk.

Here are some guidelines about simple volumes:

- ▶ You can create simple volumes on dynamic disks only.
- ▶ Simple volumes are not fault tolerant.
- ▶ Simple volumes cannot contain partitions or logical drives.

## Spanned Volumes

A spanned volume consists of disk space from more than one physical disk. You can add more space to a spanned volume by extending it at any time. To create a spanned volume, perform the following steps:

1. Open Disk Management.
2. Right-click the unallocated space on one of the dynamic disks where you want to create the spanned volume and then click **New Spanned Volume**.
3. When the Welcome to the New Spanned Volume Wizard appears, click the **Next** button.
4. Add two or more drives on the selected column. Specify the size of each volume. Click the **Next** button.
5. Specify the drive letter and click the **Next** button.
6. Specify NTFS file system and specify a volume label for easier identification. You can also specify a quick format and enable file and folder compression. Click the **Next** button.
7. When the wizard is complete, click the **Finish** button.

Here are some guidelines about spanned volumes:

- ▶ You can create spanned volumes on dynamic disks only.
- ▶ You need at least two dynamic disks to create a spanned volume.
- ▶ You can extend a spanned volume onto a maximum of 32 dynamic disks.
- ▶ Spanned volumes cannot be mirrored or striped.
- ▶ Spanned volumes are not fault tolerant.

## Extending Simple or Spanned Volumes

Simple volumes are the most basic volumes on dynamic disks. If you extend a simple volume to another dynamic disk, it automatically becomes a spanned volume. You can extend a simple volume to make it a spanned volume, and you can also further extend a spanned volume to add disk storage capacity to the volume. To extend a simple or a spanned volume, perform the following steps:

1. Open Disk Management.
2. Right-click the simple or spanned volume you want to extend, and click **Extend Volume**.
3. When the Welcome to the Extend Volume Wizard appears, click the **Next** button.
4. Select a disk that has free disk space on the Selected column and specify the amount that you want to expand. Then click the **Next** button.
5. Click the **Finish** button.

You must be a member of the Backup Operators or the Administrators group to extend or shrink any partition or volume.

You should be aware of the many rules about extending a simple or a spanned volume:

- ▶ You can extend partitions on basic disks or volumes in dynamic disks.
- ▶ You can only extend if the volume has been formatted with NTFS or raw (not formatted). You cannot extend volumes formatted using FAT or FAT32.
- ▶ After a volume is extended onto multiple disks (spanned), you cannot mirror the volume, nor can you make it into a striped volume or a RAID-5 volume.

- ▶ For logical drives, boot, or system volumes, you can extend the volume only into contiguous space and only if the disk can be upgraded to a dynamic disk. For other volumes, you can extend the volume into non-contiguous space, but you are prompted to convert the disk to dynamic.
- ▶ You can extend a logical drive within contiguous free space in the extended partition that contains it. If you extend a logical drive beyond the free space available in the extended partition, the extended partition grows to contain the logical drive.
- ▶ After a spanned volume is extended, no portion of it can be deleted without the entire spanned volume being deleted.
- ▶ You can extend simple and spanned volumes on dynamic disks onto a maximum of 32 dynamic disks.
- ▶ Spanned volumes write data only to subsequent disks as each disk volume fills up. Therefore, a spanned volume writes data to physical disk 0 until it fills up, then it writes to physical disk 1 until its available space is full, then it writes to physical disk 2, and so on. However, if just one disk fails as part of the spanned volume, *all the data contained on that spanned volume is lost*.

## Shrinking Volumes

If you are using dynamic disks, you can also shrink a volume assuming that you have enough space to hold its contents and all files can be moved out of the way if necessary. Different from expanded volumes, you can shrink the system volume.

To shrink a volume:

1. Right-click the volume and select **Shrink volume**.
2. Enter the amount of space to shrink and click the **Shrink** button.

## Striped Volumes

A striped volume stores data in stripes on two or more physical disks. Data in a striped volume is allocated alternately and evenly (in stripes) to the disks contained within the striped volume. Striped volumes can substantially improve the speed of access to the data on disk. Striped volumes are often

referred to as RAID-0; this configuration tends to enhance performance, but it is not fault tolerant. To create a striped volume, perform the following steps:

1. Open Disk Management.
2. Right-click unallocated space on one of the dynamic disks where you want to create the striped volume and select **New Striped Volume**.
3. When the Welcome to the New Striped Volume screen displays, click the **Next** button.
4. Add two disks to the Selected column, as shown in Figure 4.4. Specify the amount of the striped volume.
5. Assign the appropriate drive letter and click the **Next** button.
6. Specify **NTFS** for the file system. You should also specify a volume label for easier identification in the future. You can also choose to do a quick format and enable file and folder compression. Click the **Next** button.
7. When the wizard is complete, click the **Finish** button.

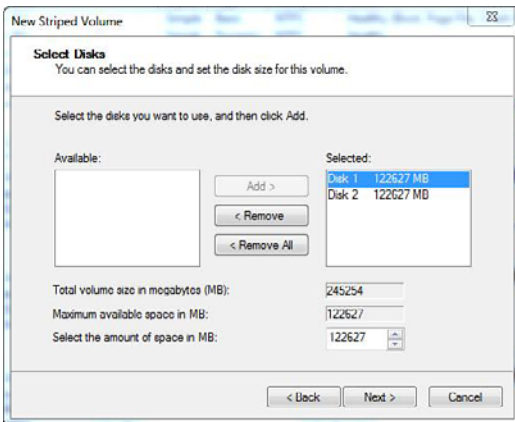


FIGURE 4.4 Selecting disks for a striped volume.

Here are some guidelines about striped volumes:

- ▶ You need at least two physical dynamic disks to create a striped volume.
- ▶ You can create a striped volume onto a maximum of 32 disks.
- ▶ Striped volumes are not fault tolerant.



- ▶ For increased volume capacity, select disks that contain similar amounts of available disk space. A striped volume's capacity is limited to the space available on the disk with the smallest amount of available space.
- ▶ Whenever possible, use disks that are the same model and from the same manufacturer.
- ▶ Striped volumes cannot be extended or mirrored. If you need to make a striped volume larger by adding another disk, you first have to delete the volume and then re-create it.

## Mirrored Volumes

A mirrored volume uses volumes stored on two separate physical disks to “mirror” (write) the data onto both disks simultaneously and redundantly. This configuration is also referred to as RAID-1. If one of the disks in the mirrored configuration fails, Windows 7 writes an event into the system log of the Event Viewer. The system functions normally (unless the second disk fails) until the failed disk is replaced and then the volume can be mirrored again. Mirrored volumes cost you 50% of your available storage space because of the built-in redundancy. If you mirror two 70 GB disks, you are left with just 70 GB of space rather than 140 GB.

You can make mirrored volumes more robust by installing a separate hard disk controller for each disk; technically, this is known as *disk duplexing*. Disk duplexing is better than disk mirroring because you alleviate the single point of failure by having one controller for each disk. Under Windows Server 2008, disk duplexing is still referred to as disk mirroring. You can create mirrored volumes only by using dynamic disks. To create a new empty mirrored volume from unallocated space, perform the following steps:

1. Open Disk Management.
2. Right-click an area of unallocated space on a dynamic disk and select **New Mirrored Volume**.
3. When the Welcome to the New Mirrored Volume Wizard starts, click **Next**.
4. Add two or more drives to the Selected column. Specify the amount of space and click the **Next** button.
5. Select the appropriate drive letter and click the **Next** button.

6. Select **NTFS** as the file system. You should also specify a volume label for easier identification. You can also select a quick format and enable file and folder compression. Click the **Next** button.
7. When the wizard is complete, click the **Finish** button.

To create a mirrored volume from a boot or system volume, or to create a mirrored volume from an existing volume that already contains data, perform the following steps:

1. Open Disk Management.
2. Right-click an existing dynamic volume and select **Add Mirror**.
3. From the window shown in Figure 4.5, select one of the available dynamic disks on which to create the redundant volume and click **Next**.

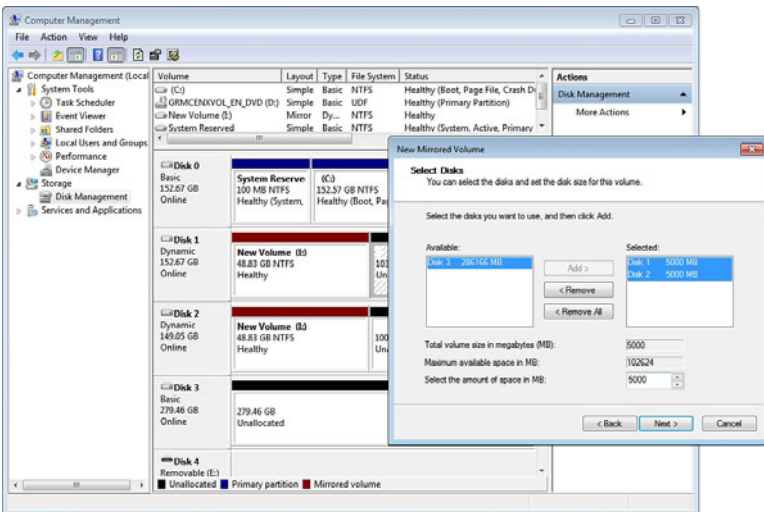


FIGURE 4.5 Creating a mirrored volume in Windows 7.

You can stop mirroring a volume by either breaking or removing the mirror. When you break a mirrored volume, each volume that makes up the mirror becomes an independent simple volume, and they are no longer fault tolerant. When you remove a mirrored volume, the removed mirrored volume becomes unallocated space on its disk, whereas the remaining mirrored volume becomes a simple volume that is no longer fault tolerant. All data that

was stored on the removed mirrored volume is erased. To break a mirrored volume, perform the following steps:

1. Open Disk Management.
2. Right-click one of the mirrored volumes that you want to break and select **Break Mirrored Volume**, as shown in Figure 4.6.
3. Click **Yes** in the Break Mirrored Volume message box.

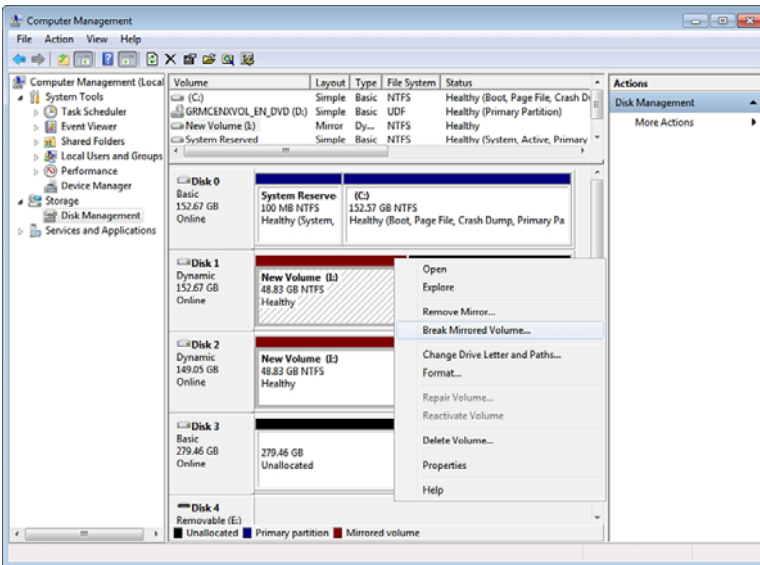


FIGURE 4.6 Breaking a mirrored volume in Windows 7.

If you want to completely destroy one of the mirrored volumes and leave just one of the volumes intact, you need to perform a removal procedure instead of simply breaking the mirrored volumes. To remove a mirrored volume, perform the following:

1. Open Disk Management.
2. Right-click a mirrored volume and then select **Remove Mirror**.
3. At the Remove Mirror dialog box, select the disk from which you want to completely erase the mirrored volume and turn the volume into unallocated space. The remaining volume stays with all of its data intact as a simple volume.

4. Click the **Remove Mirror** button.
5. Click **Yes** to confirm the removal action at the Disk Management message box that appears.

## Mount Points

When you prepare a volume in Windows 7, you can assign a drive letter to the new volume or you can create a mount point the new volume as an empty NTFS folder. By using volume mount points, you can graft, or mount, a target partition into a folder on another drive. The mounting is handled transparently to the user and applications. With the NTFS volume mount points feature, you can surpass the 26-drive-letter limitation.

To assign a mount-point folder path to a drive by using the Windows interface:

1. In Disk Manager, right-click the partition or volume where you want to assign the mount-point folder path, and then click **Change Drive Letter and Paths**.
2. To assign a mount-point folder path, click **Add**. As shown in Figure 4.7, click **Mount in the following empty NTFS folder**, type the path to an empty folder on an NTFS volume, or click **Browse** to locate it.

To remove the mount-point folder path, click it and then click **Remove**.

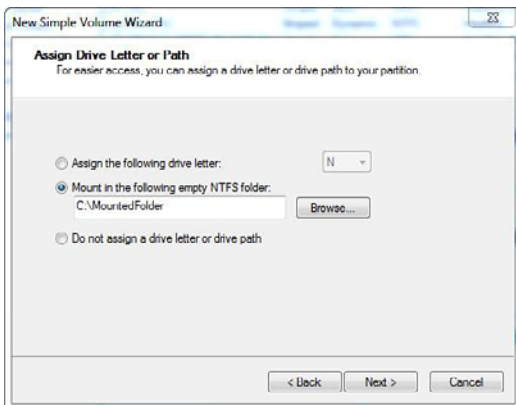


FIGURE 4.7 Mount points.

## Formatting Disks

Formatting a hard drive is the process of writing the file system structure on the disk so that it can be used to store programs and data. This includes creating a file allocation table (an index listing all directories and files and where they are located on the disk) and a root directory to start with. In addition, formatting creates a volume boot sector, which is used to store the boot files of an operating system. If you format a disk that already has a file system and files or folders, you overwrite with a new file system, which erases all content on the drive.

When you create a volume in the Disk Management console using the Add Volume Wizard, it formats the volume. However, you can format the disk any time if you want to erase all content on a volume by right-clicking the volume in the Disk Management console and selecting **Format**. You then specify a volume label, the file system, the allocation unit size, if you want to perform a quick format, and if you want to enable file and folder compression. Then click **OK**.

To format the disk using a command executed from the command prompt, you can also use the `format` command. To format the drive as D drive with an NTFS file system, you execute the following command:

```
format d: /fs:ntfs
```

---

## Cram Quiz

1. Which of the following is not supported in Windows 7?
  - A. Simple disk
  - B. Spanned disk
  - C. Mirrored disk
  - D. Striped disk
  - E. RAID-5

2. You have a Windows 7 computer. You want to provide fault tolerance for the volume containing the operating system. Each disk is configured as a basic disk. The operating system is installed on the first disk. What should you do?
- A. Configure a new mirrored volume using disk 0 and 1.
  - B. Convert both disks to a dynamic disk. Configure a new mirrored volume using disk 0 and 1.
  - C. Convert disk 1 to dynamic disks. Configure a new mirrored volume using disk 0 and 1.
  - D. Convert the disk 0 and disk 1 to dynamic disks. Configure the two disks as a striped set using disk 0 and 1.
3. Which of the following gives you the best read-access performance?
- A. Simple disk
  - B. Spanned disk
  - C. Mirrored disk
  - D. Striped disk

## Cram Quiz Answers

1. **E** is correct. Although Windows Server 2008 supports all five that are listed, Windows 7 does not support RAID-5 software RAID using Windows. You can still use hardware RAID to implement RAID-5, but this capability is not Windows 7 native. Therefore, the other answers are incorrect because they are supported in Windows 7.
2. **B** is correct. To use RAID provided by Windows 7, you must use dynamic disks. To provide fault tolerance, you create a mirrored set using disk 0 and 1. Answer A is incorrect because basic disks cannot be used for a mirror or RAID 5 disks. Answer C is incorrect because both disks must be dynamic to support mirroring and RAID-5 sets. Answer D is incorrect because a striped set is not fault tolerant.
3. **D** is correct. Striped volumes can substantially improve the speed of access to the data on disk. Striped volumes are often referred to as RAID-0; this configuration tends to enhance performance, but it is not fault tolerant. Answer C is incorrect because while mirroring does provide some increased performance and provides fault tolerance, striped disks offer faster read performance. Answers A and B are incorrect because they do not offer any increase in performance.
-

# Optimizing the Disk

## ► Manage disks

### CramSaver

1. Why do you need to keep your drives defragged?
  - A. To keep your drive from filling up
  - B. To keep your drive clean from viruses
  - C. To keep your drive optimized for better performance
  - D. To keep your drive free from disk errors
2. You have a computer running Windows 7 used by multiple users. You want to ensure that a single user does not use too much disk space on the system. What can you do?
  - A. Do not assign administrative permissions to the users
  - B. Enable disk compression
  - C. Establish disk quotas
  - D. Run the disk cleanup tool

### Answers

1. **C** is the correct because disk fragmentation leads to slow disk performance. Answers A and B are incorrect because defragging your drive does not keep the drive from filling up or clean from viruses. Answer D is incorrect because keeping a drive free from disk errors is done by **chkdsk**.
2. **C** is correct. To limit how much space a user can use, you can use disk quotas. Answer A is incorrect because not assigning administrative permissions does not prevent or limit someone who has the write permission to store files on their Desktop or Documents library. Answer B is incorrect because disk compression only provides more disk space but does not limit how much a user can use. Answer D is incorrect because the disk cleanup tool helps free up disk space to remove unnecessary files and compress old files but does not limit how much space a user can use.

One of the key components to the system is the disk. In the Windows operating system, your applications and the data come from the hard drive, so you must keep the hard drive optimized to keep your system performing well. Of course, as mentioned earlier, it is important that you use the NTFS file system. You should monitor free disk space, check your drive for errors, and defrag your hard drive on a regular basis.

## Monitoring Disk Space

You should closely monitor disk space usage on all system drives. When a system drive fills up, the performance and reliability of Windows can be greatly reduced, particularly if the system runs low on space for storing virtual memory or temporary files. One way to reduce disk space usage is to use the Disk Cleanup tool to remove unnecessary files and compress old files.

## Running Check Disk

You should periodically use the Error-checking tool to check the integrity of disks, which examines and corrects many types of common errors. You can run Check Disk (`chkdsk.exe`) from the command line. However, both methods cannot fix a corrupt file.

To test the C drive with the `chkdsk` command, you first open an elevated command prompt. You then type the following:

```
chkdsk C:
```

Without the `/f` option, Check Disk only reports the status of the C drive and any problems that it finds. To fix the problems, you need to do the following:

```
chkdsk C: /f
```

### ExamAlert

To fix errors, you must include the `/f` option with the `chkdsk` command.

To run the graphical interface of Check Disk, you do the following:

1. Click **Start** and then click **Computer**. Under Hard Disk Drives, right-click a drive and then select **Properties**.
2. On the Tools tab, click **Check now**, as shown in Figure 4.8.



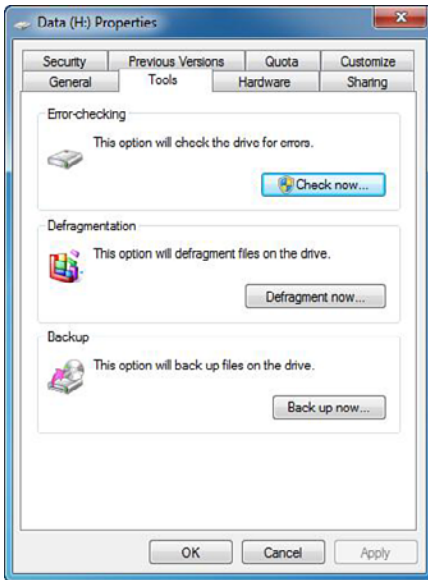


FIGURE 4.8 Disk Tools.

If you are using the command prompt or the graphical interface, you are prompted to dismount or schedule the disk to be checked the next time you restart the system.

If your machine experiences an abnormal shutdown, there is a specific bit in the registry so that when the operating system boots the next time, it knows that the file system is considered “dirty” and that it needs to be checked for possible errors. The `chkntfs` command displays or modifies automatic disk checking when the computer is started. If used without options, `chkntfs` displays the file system of the specified volume. If automatic file checking is scheduled to run, `chkntfs` displays whether the specified volume is dirty or is scheduled to be checked the next time the computer is started.

## Defragging the Hard Drive

When a file is created, it is assigned the number of clusters needed to hold the amount of data. After the file is saved to the disk, other information is usually saved to the clusters following those assigned to the saved file. Therefore, if the original file is changed or more information is added to it, the bigger file doesn't fit within the allocated clusters when it is saved back to the disk. Part of the file is saved in the original clusters and the remaining amount are placed elsewhere on the disk. Over time, files become fragmented as they are

spread across the disk. The fragmented files are still complete when they are opened, but it takes longer for the computer to read them, and opening them causes more wear and tear on the hard disk.

To reduce fragmentation, Windows 7 automatically defragments the disk periodically using Disk Defragmenter, as shown previously in Figure 4.6. By default, Windows 7 runs the disk defragmenter automatically at 1:00 A.M. every Wednesday via the Task Scheduler. As long as the computer is on at the scheduled run time, automatic defragmentation occurs. You can cancel automated defragmentation or modify the defragmentation schedule by following these steps:

1. Click **Start** and then click **Computer**.
2. Under Hard Disk Drives, right-click a drive and then select **Properties**.
3. On the Tools tab, click **Defragment Now** to open the Disk Defragmenter dialog box.
4. To cancel automated defragmentation, clear **Run Automatically** and then click **OK** twice. To modify the defragmentation schedule, click **Modify Schedule**. Use the Modify Schedule dialog box to set the desired run schedule.
5. Click **OK** twice to save your settings.

You can manually defragment a disk by completing the following steps:

1. Click **Start** and then click **Computer**.
2. Under Hard Disk Drives, right-click a drive and then select **Properties**.
3. On the Tools tab, click **Defragment Now**.

#### Note

Depending on the size of the disk, defragmentation can take several hours. You can click **Cancel Defragmentation** at any time to stop defragmentation.

## NTFS Disk Quotas

NTFS disk quotas track and control disk usage on a per-user, per-drive letter (partition or volume) basis. You can apply disk quotas only to NTFS-formatted drive letters under Windows 7. Quotas are tracked for each drive letter, even if the drive letters reside on the same physical disk. The per-user feature of quotas enables you to track every user's disk space usage regardless of which

folder the user stores files in. To enable disk quotas, open Windows Explorer or Computer, right-click a drive letter and select **Properties**, click the **Quota** tab, and configure the options, as shown in Figure 4.9.

### ExamAlert

NTFS disk quotas do not use compression to measure disk-space usage, so users cannot obtain or use more space simply by compressing their own data.

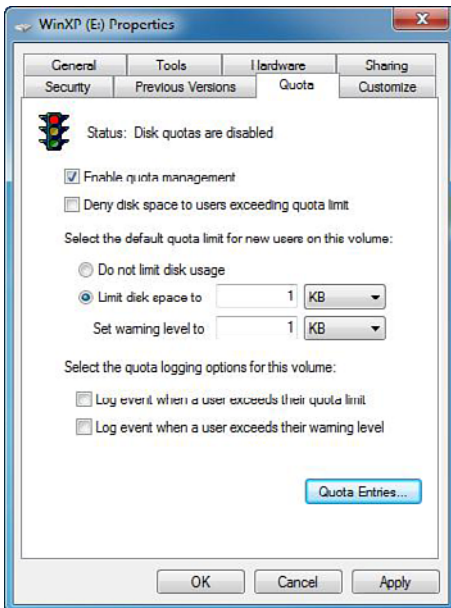


FIGURE 4.9 Configuring disk quotas.

After you turn on the disk quota system, you can establish individual disk-quota limits for each user by clicking the **Quota Entries** button at the bottom of the Quota tab. By default, only members of the Administrators group can view and change quota entries and settings. In addition, all members of the Administrators group inherit unlimited disk quotas by default. NTFS disk quotas are based on file ownership; operating system accounts are not immune to disk quotas. System accounts such as the local system are also susceptible to running out of disk space because of disk quotas having been set. From the Quota Entries window, you can change an existing quota entry for a user by double-clicking the quota entry. To set up a new quota entry for a user, click

the **Quota** menu and select the **New Quota Entry** option. When a user no longer stores data on a volume, you should delete the user's disk-quota entries. The catch is that you can only delete the user's quota entries after you remove all the files that the user owns or after another user takes ownership of the files.

---

## Cram Quiz

1. You have a computer running Windows 7 Enterprise. Unfortunately, you notice that the computer is running slowly. When you first look at it, you notice that your system has 2 GB of RAM and approximately 200 MB of free disk space. What should you do to improve performance? (Choose two answers.)
  - A. Enable your paging file
  - B. Run the Disk Defragmenter utility
  - C. Use Disk Cleanup to delete temporary files and unnecessary program files
  - D. Modify non-essential services to run in the background
2. What option do you have to use with the `chkdsk` command if you want the `chkdsk` command to fix problems that it finds?
  - A. `/c`
  - B. `/x`
  - C. `/f`
  - D. No option is required.

## Cram Quiz Answers

1. **B** and **C** are correct. You should run the Disk Defragmenter. A disk tends to become more fragmented when the disk fills up. Disk Defragmenter also helps increase performance. You should also run the Disk Cleanup program to free up additional space. Answer A is incorrect because you most likely already have a paging file. Answer D is incorrect because services already run in the background.
  2. **C** is correct. Without the `/f` option, Check Disk only reports the status of the C drive and any problems that it finds. Answer A is incorrect because the `/c` option skips checking of cycles within the NTFS folder structure. Answer B is incorrect because the `/x` option forces the volume to dismount first if necessary. Answer D is incorrect because you have to include the `/f` option.
-

# Review Questions

1. How many primary partitions does an MBR basic disk support?
  - A. 2
  - B. 4
  - C. 6
  - D. 16
  - E. 128
2. How many partitions does a GPT disk support?
  - A. 2
  - B. 4
  - C. 8
  - D. 16
  - E. 128
3. You have a Windows 7 computer with two hard drives. What type of RAID can you implement to provide fault tolerance?
  - A. RAID-0
  - B. RAID-1
  - C. RAID-5
  - D. RAID-1 and -5
4. Which of the following statements are true about basic disks under Windows 7? (Choose two.)
  - A. Basic disks are not supported under Windows 7.
  - B. Basic disks that were configured as one disk striping with parity set under Windows NT Workstation 4.0 are mounted automatically after the computer is upgraded to Windows 7.
  - C. Basic disks can only be formatted as FAT or FAT32.
  - D. You cannot convert dynamic disks back to basic disks without deleting all data and volumes on the disks first.
  - E. IEEE 1394 disks can only be basic disks.

5. You have a Windows 7 computer. What command do you use to convert a basic disk to a dynamic disk?
- A. `diskpart basic to dynamic`
  - B. `diskpart convert dynamic`
  - C. `format c: /fs:dynamic`
  - D. `convert c: /fs:dynamic`
6. What command would you use to change a master boot record disk into a GUID partition table disk?
- A. `fdisk`
  - B. `format`
  - C. `diskpart`
  - D. `convert`
7. What is the largest drive that the MBR partitioning style supports?
- A. 1 TB
  - B. 2 TB
  - C. 4 TB
  - D. 16 TB
8. Which of the following is not true when considering extending a volume?
- A. You can extend partitions on basic disks.
  - B. You can extend volumes on dynamic disks.
  - C. You cannot extend System or boot volumes.
  - D. You can only extend a volume if the volume is NTFS or raw (not formatted).
9. What is the maximum number of simple or spanned volumes that you can use on dynamic disks?
- A. 4
  - B. 8
  - C. 16
  - D. 32
10. How can you use volumes beyond the 26 drive letters?
- A. Compress the drive
  - B. Assign double letters for the drive letters
  - C. Mount the drives
  - D. Double format the drives

# Review Questions Answers

1. Answer **B** is correct. An MBR basic disk can support up to four primary partitions or three primary partitions and one extended partition. Therefore, the other answers are incorrect.
2. Answer **E** is correct. Although MBR can support up to 4 partitions, GPT can support up to 128 partitions. Therefore, the other answers are incorrect.
3. Answer **B** is correct. RAID-1, disk mirroring, uses two disks to provide fault tolerance. In RAID-1, whatever is written to one disk is written to the other. Answer A is incorrect because RAID-0, disk striping, does enhance performance, but does not provide fault tolerance. Answers C and D are incorrect because RAID-5 (disk striping with parity) needs three disks to implement. In addition, software RAID-5 is not supported on Windows 7.
4. Answers **D** and **E** are correct. To convert dynamic disks back to basic disks, you must remove all volumes on the disk, which means that all data must be removed as well. IEEE 1394 (or FireWire) disks cannot be converted to dynamic; therefore, they can only be basic disks. Answer A is incorrect because basic disks are supported under Windows 7. Answer B is incorrect because you cannot upgrade from Windows NT to Windows 7. Answer C is incorrect because basic disks (and dynamic disks) can be formatted as FAT, FAT32, or NTFS.
5. Answer **B** is correct. To convert a basic disk to a dynamic disk, you use the `diskpart convert dynamic` command. Answer A is incorrect because the proper command is `diskpart convert dynamic`. Answers C and D are incorrect because the `format` and `convert` commands cannot be used to convert basic to dynamic disks.
6. Answer **C** is correct. Diskpart is a powerful disk management tool that can convert an MBR disk to a GUID partition table disk. Answer A is incorrect because `fdisk` is a partitioning tool used in older operating systems. Format is used to format a disk, which would define FAT32 or NTFS. Answer D is incorrect because the `convert` command could be used to convert a FAT32 volume to a NTFS volume.
7. Answer **B** is correct. The largest drive that MBR partitioning style supports is 2 TB. If you need a larger drive, you have to use the GPT partitioning style.
8. Answer **C** is correct. You can extend a system or boot volume if the drive has contiguous space next to the system or boot volume and only if the disk is upgraded to dynamic disks. Answer A is incorrect because you can extend partitions on basic disks. You cannot extend logical drives, boot, or system volumes unless you convert it to dynamic disk first. Answer B is incorrect because you can extend dynamic disks. Answer D is incorrect because you can only extend NTFS or raw partitions. You cannot extend FAT or FAT32 volumes.
9. Answer **D** is correct. You can extend simple and spanned volumes on dynamic disks onto a maximum of 32 dynamic disks. Therefore, the other answers are incorrect.

10. Answer **C** is correct. When you prepare a volume in Windows 7, you can assign a drive letter to the new volume or you can create a mount point, and then you assign the new volume to an empty NTFS folder. By using volume mount points, you can graft, or mount, a target partition into a folder on another drive. The mounting is handled transparently to the user and applications. With the NTFS volume mount points feature, you can surpass the 26-drive-letter limitation. Answer A is incorrect because compressing the drive only gives you more space on the drive. Answer B is incorrect because you cannot assign double letters. Answer D is incorrect because there is no such thing as double formatting a drive.



*This page intentionally left blank*

## CHAPTER 5

# Configuring Windows Networking

### **This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Network Connectivity:
  - ▶ Configure IPv4 network settings
  - ▶ Configure IPv6 network settings
  - ▶ Configure networking settings

A network is two or more computers connected to share resources such as files or printers. To function, a network requires a service to share (such as file or print sharing) and access to a common medium or pathway. Today, most computers connect to a wired network using an Ethernet adapter, which in turn connects to a switch or set of switches via a twisted pair cable, or the computers connect to a wireless network using a wireless adapter to connect to a wireless switch. To bring it all together, protocols give the entire system common communication rules. Today, virtually all networks use the TCP/IP protocol suite, the same protocol that the Internet runs.

# Introduction to TCP/IP

- ▶ **Configure IPv4 network settings**
- ▶ **Configure IPv6 network settings**
- ▶ **Configure networking settings**

## CramSaver

1. What is the default subnet mask for the host address of 172.1.32.4?

- A.** 255.0.0.0
- B.** 255.255.0.0
- C.** 255.255.255.0
- D.** 255.255.255.255

2. You have the following addresses:

Server01 (DNS Server): 172.24.1.30

Server02 (WINS Server): 172.24.2.31

Server03 (DHCP Server): 172.24.2.60

Server04 (DC): 172.24.2.61

Router: 172.24.2.1

Which address should your default gateway point to?

- A.** 172.24.1.30
- B.** 172.24.2.31
- C.** 172.24.2.60
- D.** 172.24.2.61
- E.** 172.24.2.1

3. What do you call the following:

2001::efd3:934a:42a2

- A.** MAC address
- B.** DNS Suffix address
- C.** WEP key
- D.** IPv4 address
- E.** IPv6 address

**Answers**

1. **B** is correct. The 172.1.32.4 address is a Class B address and a private address. The default subnet mask for a Class B address is 255.255.0.0. Answer A is incorrect because the 255.0.0.0 mask is used for a Class A network that has the first octet beginning with 1 to 126. Answer C is incorrect because the 255.255.255.0 mask is used for a Class C network that has the first octet beginning with 192 to 223. Answer D is incorrect because the 255.255.255.255 mask is used to specify that the address is the only one included and is not part of a range.
2. **E** is correct. The default gateway should point to a router so that it knows where to forward packets that need to be sent to remote subnets. Therefore, the other answers are incorrect.
3. **E** is correct. The 2001::efd3:934a:42a2 address is an IPv6 address. This address is short for 2001:0000:0000:0000:efd3:934a:42a2. Therefore, the other answers are incorrect.

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry suite of protocols on which the Internet is based. It is supported by all versions of Windows and virtually all modern operating systems. The TCP/IP protocol suite operates on top of the networking physical layer, such as Ethernet and 802.11 wireless networks.

The lowest level protocol within the TCP/IP model (not to be confused with the OSI model) is the Internet protocol (IP), which is primarily responsible for addressing and routing packets between hosts. Each connection on a TCP/IP address is called a *host* (a computer or other network device that is connected to a TCP/IP network) and is assigned a unique IP address. A host is any network interface, including each network's interface cards or a network printer that connects directly onto the network. When you send or receive data, the data is divided into little chunks called packets. Each of these packets contains both the sender's TCP/IP address and the receiver's TCP/IP address.

Windows 7 supports both IPv4 and IPv6 through a dual-IP-layer architecture and enables both by default. This architecture enables you to tunnel IPv6 traffic across an IPv4 network in addition to tunneling IPv4 traffic across an IPv6 network.

## IPv4 TCP/IP Addressing

When you talk about networking, you have to use addressing to identify a host on the network. All hosts use physical addresses known as Media Access Control (MAC) addresses. Most network interfaces have their MAC addresses

burned onto a chip and cannot be changed. These addresses are 48-bits and are expressed in hexadecimal format with colons or dashes:

00-C0-9F-8E-82-00

Much like a host address, you cannot have two hosts with the same MAC address on the same physical network. The Address Resolution Protocol (ARP) translates from logical addresses to the MAC addresses, which can be viewed with the `arp.exe` command from a command prompt.

The traditional version of the IP protocol is version 4—IPv4. Each connection on a TCP/IP network is assigned a unique IP address. An IPv4 address is a logical address that is managed and organized by a network administrator. The format of the IP address is four 8-bit numbers (octets) divided by periods (.). Each number can be 0 to 255. For example, a TCP/IP address could be 131.107.3.1 or 2.0.0.1.

IP addresses are manually assigned and configured (static IP addresses) or dynamically assigned and configured by a Dynamic Host Configuration Protocol (DHCP) server (dynamic IP addresses). Because the IP address is used to identify the computer, no two connections can use the same IP address; otherwise, one or both of the computers would not be able to communicate, which usually results in a message stating “IP address conflict.”

The TCP/IP address is broken down into a network number and a host number. The network number identifies the entire network and the host number identifies the computer or connection on the specified network.

Usually when defining the TCP/IP for a network connection, IT managers also specify a subnet mask. A subnet mask is used to define which address bits describe the network number and which address bits describe the host address. Similar to the IP address, the format of the subnet mask is four 8-bit numbers (octet) divided by periods (.). Each number can be 0 to 255. For example, a subnet mask could be 255.0.0.0, 255.255.255.0, or 255.255.240.0.

For example, if you have an address of 15.2.3.6 and you define a subnet mask of 255.255.255.0, 15.2.3.0 defines the network address where every computer on that network must begin with 15.2.3. Then each computer must have a unique host number, making the entire address unique. Because the first three octets are defined as the network ID, the last octet defines the host ID. Therefore, one host (and only one host) has a host ID of 0.0.0.6 located on the 15.2.3.0 network.

In simple IPv4 networks, the subnet mask defines full octets as part of the network ID and host ID. Table 5.1 lists the characteristics of each IP address class.

TABLE 5.1 IP Address Classes

Class	First Octet	Default Subnet Mask	Number of Networks	Number of Hosts per Network
A	1–126	255.0.0.0	126	16,777,214
B	128–191	255.255.0.0	16,384	64,534
C	192–223	255.255.255.0	2,097,152	254

The loopback address (127.0.0.1) is a special designated IP address (127.0.0.1) that is designated for the software loopback interface of a machine and is used to test IP software. In addition, if you access localhost, you are accessing the loopback address of 127.0.0.1.

Unfortunately, using classes to define networks allows for a lot of wasted addresses. To make use of these wasted addresses, classless addresses, or Classless Inter-Domain Routing (CIDR), was developed to not use the specific Class A, B, and C. Because CIDR does not use assign a Class A network address to a corporation or some other organization, it does not waste 16 million addresses. Instead, what would normally be a Class A address can be divided and given to multiple companies and organizations.

Because there are no classes that have a default subnet mask, CIDR subnetting uses a different notation that defines how many bits are masked. For example, if you had a subnet mask of 255.255.255.0, you use a CIDR notation of /24. The 24 is because the first 24 bits are masked (11111111.11111111.11111111.00000000). Therefore, an address is designated as

192.168.1.1/24

If an individual network is connected to another network and users must communicate with any computers on the other network, they must also define the default gateway, which specifies the local address of the router. If the default gateway is not specified, users are not able to communicate with computers on other networks. If the LAN is connected to more than two networks, users must specify only one gateway, because when a data packet is sent, the gateway first determines if the data packet needs to go to a local computer or onto another network. If the data packet is meant to be sent to a computer on another network, the gateway forwards the data packet to the router. The router then determines the best direction that the data packet must go to reach its destination.

If you are connected to the Internet, you need a default gateway. Because the default gateway address is an address of a host, it also is four 8-bit numbers

(octet) divided by periods (.). Each number can be 0 to 255. Because it must be connected on the same network as the host, it must also have the same network address as the host address.

Because TCP/IP addresses are scarce for the Internet (based on the IPv4 and its 32-bit addresses), a series of addresses have been reserved to be used by the private networks. These addresses can be used by many organizations because these addresses are not seen from outside of the local network. The private IPv4 addresses are as follows:

- ▶ 10.x.x.x (1 Class A address range)
- ▶ 172.16.x.x to 172.31.x.x (16 Class B address ranges)
- ▶ 192.168.0.x to 192.168.255.x (256 Class C address ranges)

To allow for these addresses to connect to the Internet, you use a router that supports Network Address Translation (NAT), also known as “IP Masquerading,” which translates between the internal private addresses and the public Internet addresses.

## IPv6 TCP/IP Addressing

The Internet has grown and continues to grow at an exponential rate. Eventually the Internet will run out of network numbers. Therefore, a new IP protocol called IPv6 is replacing IPv4.

IPv6 provides a number of benefits for TCP/IP-based networking connectivity, including

- ▶ **Large address space:** The 128-bit address space for IPv6 potentially provides every device on the Internet with a globally unique address.
- ▶ **Efficient routing:** The IPv6 network packet supports hierarchical routing infrastructures, which enables more efficient routing than IPv4.
- ▶ **Straightforward configuration:** IPv6 can use both DHCP for IPv6 (DHCPv6) and local routers for automatic IP configuration.
- ▶ **Enhanced security:** The IPv6 standard provides better protection against address and port scanning attacks and all IPv6 implementations support IPsec for protection of IPv6 traffic.

IPv4 is based on 32-bit addresses (four 8-bit octets), which allows a little more than 4 billion hosts. IPv6 uses 128 bits for the addresses, which can have up to  $3.4 \times 10^{38}$  hosts. Thus, IPv6 can handle all of today’s IP-based machines and

allow for future growth while handling IP addresses for mobile devices such as personal digital assistants (PDAs), cell phones, and similar smart devices.

An IPv6 address is divided into groups of 16 bits, written as four hex digits. Hex digits include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F. The groups are separated by colons. An example of an address is

```
FE80:0000:0000:0000:02A0:D2EF:FEA5:E9F5
```

Similar to IPv4, the IPv6 addresses are split in two parts: bits that identify the network and bits that define the host address. Different from IPv4, IPv6 has a fixed prefix that contains specific routing and subnet information. The first 64 bits (four groups of four hex digits) define the network address and the second 64 bits define the host address. For the address of FE80:0000:0000:0000:02A0:D2EF:FEA5:E9F5, FE80:0000:0000:0000 defines the network bits and 02A0:D2EF:FEA5:E9F5 defines the host bits.

While IPv6 addresses are expressed with hexadecimal digits, a 128-bit address still uses 32 hexadecimal digits. Therefore, in some situations, you can abbreviate an IPv6 address. When an IPv6 address has two or more consecutive eight-bit blocks of zeroes, you can replace them with a double colon, as follows:

```
42cd:0051:0000:0000:c8ba:03f2:003d:b291
```

This becomes

```
42cd:0051::c8ba:03f2:003d:b291
```

You can also remove the leading zeros in any block. Therefore, for our example, you have

```
42cd:51::c8ba:3f2:3d:b291
```

The IPv6 address types include the following:

- ▶ **Unicast:** Used for one-to-one communication between hosts. Each IPv6 host has multiple unicast addresses. The Unicast IPv6 can be further broken down to
  - ▶ **Global Unicast address:** Addresses that are equivalent to IPv4 public addresses so they are globally routable and reachable on the IPv6 portion of the Internet. Global Unicast addresses start with a 2 or 3.
  - ▶ **Link-Local addresses:** Used by hosts when communicating with neighboring hosts on the same link. They are equivalent to IPv4 APIPA addresses and start with FE8.



- ▶ **Unique local unicast addresses:** Equivalent to IPv4 private address spaces and start with FEC0.
- ▶ **Multicast:** Used for one-to-many communication between computers that are defined as using the same multicast address.
- ▶ **Anycast address:** An IPv6 unicast address that is assigned to multiple computers. When IPv6 addresses communicate to an anycast address, only the closest host responds. You typically use this for locating services or the nearest router.

The last 64-bits of an IPv6 address are the interface identifier. This is equivalent to the host ID in an IPv4 address. Each interface in an IPv6 network must have a unique interface identifier. Some network implementations use EUI-64, which derives the last 64-bits based on the MAC address.

Because the interface identifier is unique to each interface, IPv6 uses it rather than media access control (MAC) addresses to identify hosts uniquely. Because the MAC address can partially be used to uniquely identify a computer, some IPv6 implementations generate a unique interface identifier to preserve privacy in network communication rather than using the network adapter's MAC address.

In the next-generation Internet Protocol, IPv6, ARP's functionality is provided by the Neighbor Discovery Protocol (NDP). NDP is responsible for

- ▶ Address autoconfiguration of nodes
- ▶ Discovery of other nodes on the link
- ▶ Determining the Link Layer addresses of other nodes
- ▶ Duplicate address detection
- ▶ Finding available routers and Domain Name System (DNS) servers
- ▶ Address prefix discovery
- ▶ Maintaining reachability information about the paths to other active neighbor nodes

### ExamAlert

If you need to assign a computer directly to the Internet, you should configure the computer with an IPv6 address that is equivalent to a public IPv4 address, which is a global unicast IPv6 address. These addresses are globally routable and can be reached from the Internet. However, computers running Windows 7 are usually connected through your ISP, which is automatically assigned an IPv6 address.

Similar to the loopback address of 127.0.0.1 used for testing, IPv6 uses 0:0:0:0:0:0:0:1. To abbreviate this address, you can write it as ::1.

Because most networks use IPv4, there are several methods that were created to transition from IPv4 to IPv6. Windows 7 and Windows Server 2008 R2 support the following methods:

- ▶ **IPv4-compatible address:** 0:0:0:0:0:w.x.y.z or ::w.x.y.z (where w.x.y.z is the dotted decimal representation of a public IPv4 address) is used by IPv6/IPv4 nodes that are communicating using IPv6. The address format consists of 96 bits of zeroes, followed by an IPv4 address in its standard dotted-decimal notation. As a result, an IPv4-compatible address is used as an IPv6 destination. The IPv4 is automatically encapsulated with an IPv6 header and sent to the destination using the IPv4 infrastructure. An example is ::192.168.1.20.
- ▶ **IPv4-mapped address:** The IPv4-mapped IPv6 address has its first 80 bits set to zero, the next 16 set to one, and the last 32 bits represent the IPv4 address. For example, ::FFFF:C000:280 is the mapped IPv6 address for 192.0.2.128. Remember, the 192.0.2.128 is written in decimal format, while the C000:280 is written in hexadecimal format. The IPv4-mapped IPv6 addresses always identify IPv4-only nodes. An example is ::ffff:192.168.1.20.
- ▶ **6to4 address:** A tunneling technology that enables computers to transmit IPv6 packets over an IPv4 network. The 6to4 address is formed by combining the prefix 2002::/16 with the 32 bits of a public IPv4 address, forming a 48-bit prefix. An example using the 192.168.1.20 IPv4 address appears as follows: 2002:C0A8:0114::/16. 6to4 is enabled by default on machines running Windows 7.
- ▶ **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) address:** Used between two unicast nodes running both IPv4 and IPv6 over an IPv4 routing infrastructure. ISATAP addresses use the locally administered interface ID ::0:5EFE:w.x.y.z, where w.x.y.z is any unicast IPv4 address, which includes both public and private addresses. The ISATAP interface ID can be combined with any 64-bit prefix that is valid for IPv6 unicast addresses. This includes the link-local address prefix (FE80::/64), site-local prefixes, and global prefixes. ISATAP is enabled by default on machines running Windows 7.
- ▶ **Teredo address:** Teredo tunneling enables you to tunnel across the IPv4 network when the clients are behind an IPv4 NAT. Teredo was created because many IPv4 routers use NAT to define a private address

space for corporate networks. For two Windows-based Teredo clients, the most crucial Teredo processes are those that you use for initial configuration and communication with a different site's peer. Teredo addresses use the prefix 2001:0000::/32. Beyond the first 32 bits, Teredo addresses are used to encode the IPv4 address of a Teredo server, flags, and the encoded version of the external address and port of a Teredo client. An example of a Teredo address is 2001:0000:9d36:b007:8000:82ff:3f57:e00c. Teredo is enabled by default on machines running Windows 7.

## Default Gateway

A default gateway is a device, usually a router, that connects the local network to other networks. When you need to communicate with a host on another subnet, you forward all packets to the default gateway. The router then determines the best way to get to the remote subnet and forwards the packets toward the remote subnet.

## Name Resolution

Most users find the IPv4 and IPv6 addresses difficult to remember when communicating with other computers. Instead, a user specifies a recognizable name, and the name is translated into an address. For example, when a user opens Internet Explorer and specifies `http://www.microsoft.com`, the `www.microsoft.com` is translated into an IP address. The web page is then accessed from the server using the translated IP addresses.

Fully Qualified Domain Names (FQDNs), sometimes referred to as just *domain names*, are used to identify computers on a TCP/IP network. Examples include the following:

`www.microsoft.com`

`www.intel.com`

`server1.acme.com`

One way to translate the FQDN to the IP address is to use a DNS server. DNS is a distributed database (a database contained in multiple servers) containing host name and IP address information for all domains on the Internet. For every domain, there is a single authoritative name server that contains all DNS-related information about the domain. When you configure IP configurations, you need to specify the address of a DNS server so that you use the Internet or log in to a Windows Active Directory domain.

For DNS to keep track of specific information, the DNS server uses resource records to hold the information. The most common resource records are the following:

- ▶ **Address record (A):** Used to resolve host names into a 32-bit IPv4 addresses.
- ▶ **IPv6 address record (AAAA):** Used to resolve host names into a 128-bit IPv6 address.
- ▶ **Pointer record (PTR):** Used to resolve IP address into a host name (reverse DNS lookup.)
- ▶ **Mail exchange record (MX):** Used to identify the mail transfer agent for an organization.
- ▶ **Service locator (SRV):** Used to identify generalized service location record, including finding the domain controllers.

Because an organization could have hundreds or even thousands of hosts, Dynamic DNS was created to register automatically a host name and IP address to a DNS server.

Besides the DNS server, a HOSTS file on each machine can also be used to translate domain/host names to IP addresses. The disadvantage of using HOSTS files is that you must add entries on every machine; however, a HOSTS file can come in handy when you want to connect to a test machine that you do not want to become widely available to everyone else.

Another naming scheme used on TCP/IP networks is using the NetBIOS names (such as that is used to identify share names for files and printers \\COMPUTERNAME\SHARENAME). To translate NetBIOS names to IP addresses, you use a Windows Internet Name Service (WINS) server or the LMHOSTS files.

#### Note

On Windows machines, the HOSTS and LMHOSTS files are located in the C:\Windows\System32\drivers\etc folder.

If you try to access a network resource by name instead of IP address and the device cannot be found, it is most likely a problem with the DNS server/HOSTS file or the WINS server/LMHOSTS file. Either the servers cannot be contacted, or the servers or files have the wrong address associated with the name. The failure of these servers or files can also affect network applications that need to access various services or resources.

For computers with IPv6 link-local addresses that do not have access to a DNS server, the system uses the Link Local Multicast Name Resolution (LLMNR) protocol. LLMNR automatically transmits name query request messages as multicast to the local network. The computer with the requested name then replies with a message containing its IP address using a unicast packet.

## DHCP Services

The Dynamic Host Configuration Protocol (DHCP) is used to automatically configure a host during boot-up on a TCP/IP network and to change settings while the host is attached. DHCP can automatically set many parameters with the DHCP server for IPv4 and IPv6 networks, which prevents network administrators from having to manually configure hundreds or even thousands of computers. Some of the more common parameters include the following:

- ▶ IP address
- ▶ Subnet mask
- ▶ Gateway (router) address
- ▶ Address of DNS server
- ▶ Address of WINS servers
- ▶ WINS client mode

IP Automatic Configuration is a method of assigning an IPv6 address to an interface automatically. It can be stateful or stateless:

- ▶ Stateful addresses are assigned by a DHCP service on a server or other device. The service that allocated the address to the client manages the stateful address.
- ▶ Stateless addresses are configured by the client and are not maintained by a service. The record of the address assignment is not maintained. Instead, the computer configures its own address after transmitting router solicitation multicasts to the routers and receives routing advertisement messages in return.

The link-local address is a stateless address that is automatically generated. It is used by the host to communicate with other hosts on the local network. A link-local address is not routable and cannot be used to communicate with hosts on a remote network. When the host generates the link-local address, the host also performs duplicate address detection to ensure that it is unique.

## IP Configuration on Windows 7 Machines

To configure the IP configuration in Windows 7, do the following:

1. Open the Control Panel.
2. While in Category view, click **Network and Internet**, click **Network and Sharing Center**, and click **Change adapter settings**.
3. Right-click the connection that you want to change and then click **Properties**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click the **Networking** tab. Under **This connection uses the following items**, click either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties** to display the resulting window in Figure 5.1.

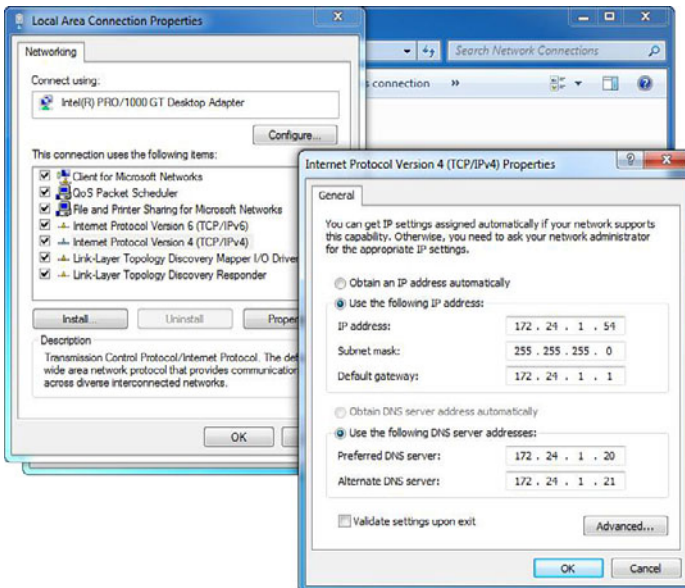


FIGURE 5.1 Configure IPv4 settings in Windows 7.

To specify IPv4 IP address settings, do one of the following:

- ▶ To obtain IP settings automatically from a DHCP server, click **Obtain an IP address automatically** and then click **OK**.
- ▶ To specify an IP address, click **Use the following IP address**, and then, in the IP address, Subnet mask, and Default gateway boxes, type the IP address settings.

To specify IPv6 IP address settings, do one of the following (see Figure 5.2):

- ▶ To obtain IP settings automatically, click **Obtain an IPv6 address automatically** and then click **OK**.
- ▶ To specify an IP address, click **Use the following IPv6 address**, and then, in the IPv6 address, Subnet prefix length, and Default gateway boxes, type the IP address settings.

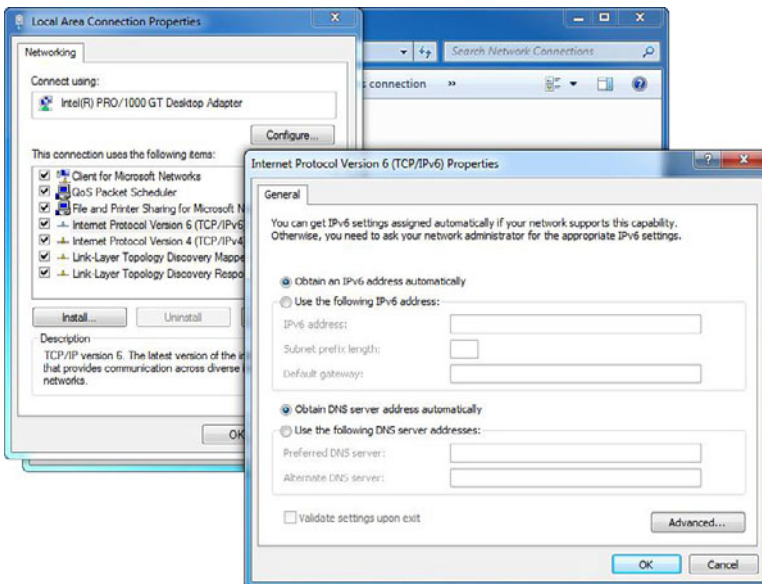


FIGURE 5.2 Configure IPv6 settings in Windows 7.

Windows 7 provides the capability to configure alternate IP address settings to support connecting to different networks. Although static IP addresses can be used with workstations, most workstations use dynamic or alternative IP addressing, or both. You configure dynamic and alternative addressing by completing the following steps:

1. Open the Control Panel.
2. While in Category view, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage Network Connections**.

### Note

Some versions of Windows 7 use Change Adapter Settings instead of Manage Network Connections.

3. Right-click the connection that you want to change and then click **Properties**.
4. Double-click **Internet Protocol Version 6 (TCP/IPv6)** or **Internet Protocol Version 4 (TCP/IPv4)** as appropriate for the type of IP address you are configuring.
5. Select **Obtain an IPv6 address automatically** or **Obtain an IP address automatically** as appropriate for the type of IP address you are configuring. If desired, select **Obtain DNS server address automatically**. Or select **Use the following DNS server addresses** and then type a preferred and alternate DNS server address in the text boxes provided.
6. When you use dynamic IPv4 addressing with desktop computers, you should configure an automatic alternative address. To use this configuration, from the Alternate Configuration tab, select **Automatic Private IP Address**. Click **OK** twice, click **Close**, and then skip the remaining steps.
7. When you use dynamic IPv4 addressing with mobile computers, you usually want to configure the alternative address manually. To use this configuration, on the Alternate Configuration tab, select **User Configured**. Then in the IP Address text box, type the IP address you want to use. The IP address that you assign to the computer should be a private IP address, and it must not be in use anywhere else when the settings are applied.
8. With dynamic IPv4 addressing, complete the alternate configuration by entering a subnet mask, default gateway, DNS, and WINS settings. When you're finished, click **OK** twice and then click **Close**.

To specify DNS server address settings for IPv4 and IPv6, do one of the following:

- ▶ To obtain a DNS server address automatically, click **Obtain DNS server address automatically** and then click **OK**.
- ▶ To specify a DNS server address, click **Use the following DNS server addresses**, and then, in the Preferred DNS server and Alternate DNS server boxes, type the addresses of the primary and secondary DNS servers.



## Network and Sharing Center

As shown in Figure 5.3, the Network and Sharing Center provides real-time status information about your network. You can see if your computer is connected to your network or the Internet, the type of connection, and what level of access you have to other computers and devices on the network. This information can be useful when you set up your network or if you have connection problems. You can find more detailed information about your network in the network map, which is accessible from the Network and Sharing Center. You can access the Network and Sharing Center from the Control Panel or from the Notification Area. You can also use the Network and Sharing Center to set up a wireless or VPN connection; create and manage homegroups; and manage a system's sharing options.

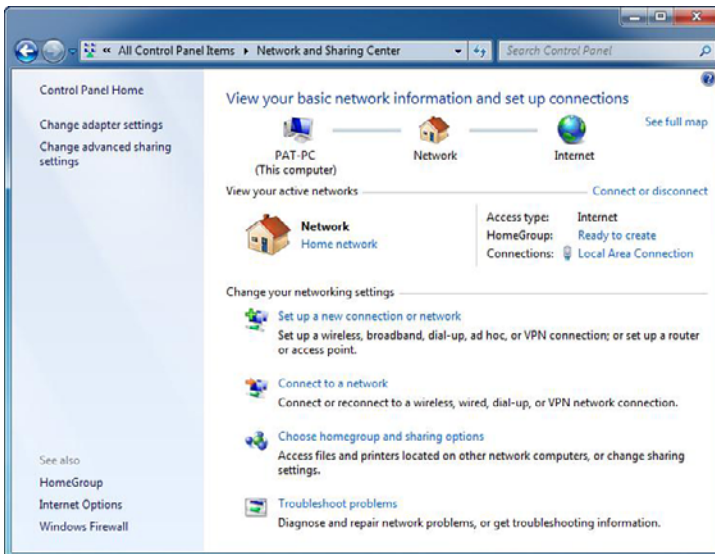


FIGURE 5.3 The Network and Sharing Center.

## Using the netsh Command

Netsh.exe is a tool an administrator can use to configure and monitor various networking parameters using the command prompt, including

- ▶ Configuring IP addresses, default gateway, and DNS servers
- ▶ Configuring interfaces
- ▶ Configuring routing protocols

- ▶ Configuring filters
- ▶ Configuring routes
- ▶ Configuring remote access behavior for Windows-based remote access servers that are running the Routing and Remote Access Server (RRAS) Service
- ▶ Displaying the configuration of a currently running router
- ▶ Using the scripting feature to run a collection of commands in batch mode against a specified router

To display the available options for the `netsh` command, you enter the following at the command line:

```
netsh /?
```

To view your interfaces, execute the following command:

```
netsh interface ipv4 show interfaces
```

When you view the output of the `netsh` command, you need to note the names of the interfaces for your network adapter.

To set a static IP address and default gateway, you use the following command:

```
netsh interface ipv4 set address name "interface name" source=static  
address=preferred IP address mask=SubnetMask gateway=gateway address
```

If you are using and configuring IPv6, you specify `ipv6` instead of `ipv4`. If the interface name includes spaces, you need to surround the name with quotes (“”). If you don’t want to assign a gateway, you specify `gateway=none`.

To set the static DNS address, use the following command:

```
netsh interface ipv4 add dnsserver name="interface name" address=IP  
address of the primary DNS server index=1
```

For each DNS server that you want to set, increment the `index= number` each time. Therefore, for the first DNS server, index would be 1. For the second DNS server, index would be 2.

To change a server to the DHCP-provided IP address from a static IP address, use the following command:

```
netsh interface ipv4 set address name="interface name" source=DHCP
```

For more information about using the `netsh` command, use the following websites:

[http://technet.microsoft.com/en-us/library/cc754516\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc754516(WS.10).aspx)

[http://technet.microsoft.com/en-us/library/cc770948\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc770948(WS.10).aspx)

---

## Cram Quiz

1. What are the two services that provide name resolution? (Choose two answers.)

- A. DNS
- B. DHCP
- C. WINS
- D. NAT

2. What command do you use to view your IPv4 interfaces on a computer running Windows 7?

- A. `netsh interface ipv4 show interfaces`
- B. `netsh interface ipv4 set address name all`
- C. `netsh interface ipv4 add interface`
- D. `netsh interface ipv4 set address name source=DHCP`

3. What IPv6 address is used to communicate with neighboring hosts on the same link?

- A. Global unicast
- B. Link-local
- C. Unique local unicast
- D. Multicast

## Cram Quiz Answers

- 1. A and C** are correct. DNS is short for Domain Name System and WINS is short for Windows Internet Name Service. DNS translates from host names/domain names to IP addresses and WINS translates from NetBIOS names/computer names. Answer B is incorrect because DHCP (short for Dynamic Host Configuration Protocol) is used to assign IP addresses automatically. Answer D is incorrect because NAT, short for Network Address Translation, is used to connect a private network through a single public address.
  - 2. A** is correct. To view your interfaces, execute the following command: `netsh interface ipv4 show interfaces`. Answers B, C, and D are incorrect because the `set` option and `add` option are used to modify or add an address, not view an address.
  - 3. B** is correct. A link-local address is used by hosts when communicating with neighboring hosts on the same link. Answer A is incorrect because the global unicast addresses are equivalent to IPv4 public addresses, so they are globally routable and reachable on the IPv6 portion of the Internet. Answer C is incorrect because the unique local unicast addresses are equivalent to IPv4 private address spaces. Answer D is incorrect because a multicast address is used for one-to-many communications between computers.
-

# Tools to Help Diagnose Network Problems

- ▶ **Configure IPv4 network settings**
- ▶ **Configure IPv6 network settings**
- ▶ **Configure networking settings**

## CramSaver

1. You had to move a well-used server to a different subnet and change the IP address. Now users are complaining that they cannot access the server. What should you do?
  - A. Have the users run the `ipconfig /all` command
  - B. Have the users run the `ipconfig /flushdns` command
  - C. Have the users change their DNS server to the new address of the server they are trying to connect to
  - D. Have the users run the `netsh interface ip set dns` command
  
2. You have a computer running Windows 7. You just configured your DHCP server to assign IPv6 addresses. What can you do to verify the addresses? (Choose two answers.)
  - A. Run the `net config` command at a command prompt
  - B. Select Details from the network connection status
  - C. Select Internet Protocol version 6 (TCP/IP) and then properties from network connection properties
  - D. Run the `NetStat` command at a command prompt
  - E. Run the `ipconfig /all` command at a command prompt

## Answers

1. **B** is correct. The `ipconfig /flushdns` command clears out the users' DNS cache so they can then retrieve the new IP address when they access the server by name. Answer A is incorrect because the `ipconfig /all` command only displays the configuration. Answer C is incorrect because changing the DNS address to the new server prevents the computers from performing DNS resolution, including the name resolution to the server, because the new server is most likely not a DNS server, which would be incapable of providing name resolution for the client PC. Answer D is incorrect because it also changes the DNS settings at a command prompt, which prevents the computer from performing DNS resolution, including the name resolution to the server, because the new server is

most likely not a DNS server, which would be incapable of providing name resolution for the client PC.

2. **B** and **E** are correct. To see what addresses are assigned to a computer, you can select Details from the network connection status or use the `ipconfig /all` command. Answer A is incorrect because the `net config` command displays the configurable workstation and server services that are running. Answer C is incorrect because the Internet Protocol version 6 (TCP/IP) only allows you to specify static addresses or to use a DHCP address. If you select to use DHCP, it does not show you the actual TCP/IP address. Answer D is incorrect because the `netstat` command is used to display protocol statistics and current TCP/IP network connections.

You can use several utilities to test and troubleshoot the TCP/IP network.

If you experience network connectivity problems while using Windows 7, you can use Window Network Diagnostics to start the troubleshooting process. If there is a problem, Windows Network Diagnostics analyzes the problem and, if possible, presents a solution or a list of possible causes. To start the Windows Network Diagnostics program, right-click the Network and Sharing Center and select Troubleshoot problems.

Windows Network Diagnostics might be able to complete the solution automatically or might require the user to perform steps in the resolution process. If Windows Network Diagnostics cannot resolve the problem, you should follow a logical troubleshooting process using tools available in Windows 7. Table 5.2 outlines some of these tools. Although some of these tools have new options to accommodate IPv6, these tools have been around for years. The `ipconfig` command shows a computer's current configuration while `ping`, `tracert`, and `pathping` are used to test network connectivity. `NSlookup` is used to test DNS name resolution.

TABLE 5.2 **Windows 7 TCP/IP Troubleshooting Tools**

Tool	Functionality
<code>ipconfig</code>	<p>The <code>ipconfig</code> command displays current TCP/IP configuration as shown in Figure 5.4.</p> <ul style="list-style-type: none"> <li>▶ <code>ipconfig /all</code> command displays full TCP/IP configuration information, as shown in Figure 5.5.</li> <li>▶ <code>ipconfig /release</code> releases the IPv4 address configured by a DHCP server.</li> <li>▶ <code>ipconfig /release6</code> releases the IPv6 address configured by a DHCP server.</li> </ul>

TABLE 5.2 **Continued**

Tool	Functionality
	<ul style="list-style-type: none"> <li>▶ <code>ipconfig /renew</code> renews the IPv4 address configured by a DHCP server.</li> <li>▶ <code>ipconfig /renew6</code> renews the IPv6 address configured by a DHCP server.</li> <li>▶ <code>ipconfig /flushdns</code> purges the DNS resolver cache.</li> <li>▶ <code>ipconfig /registerdns</code> refreshes all DHCP leases and re-registers DNS names.</li> </ul>
ping	<p>By using the ICMP protocol, the <code>ping</code> command verifies connections to a remote computer by verifying configurations and testing IP connectivity.</p> <ul style="list-style-type: none"> <li>▶ The <code>-t</code> option pings the specified host until stopped.</li> <li>▶ The <code>-a</code> option resolves address to host name.</li> <li>▶ The <code>-S srcaddr</code> option specifies the source address to use.</li> <li>▶ The <code>-4</code> option forces the ping command to use IPv4.</li> <li>▶ The <code>-6</code> option forces the ping command to use IPv6.</li> </ul>
tracert	<p>The <code>tracert</code> command traces the route that a packet takes to a destination and displays the series of IP routers that are used in delivering packets to the destination. If the packets are unable to be delivered to the destination, the <code>tracert</code> command displays the last router that successfully forwarded the packet. The <code>tracert</code> command also uses the ICMP protocol.</p>
pathping	<p><code>pathping</code> traces a route through the network in a manner similar to <code>tracert</code>. However, <code>pathping</code> also provides more detailed statistics on the individual hops.</p>
nslookup	<p>The <code>nslookup</code> command displays information that you can use to diagnose your DNS infrastructure. You can use <code>nslookup</code> to confirm connection to the DNS server and the existence of required resource records.</p>

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\patrickreg>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . : hsd1.ca.comcast.net.
    IPv6 Address. . . . . : 2001:db8::2aa:ff:f328:9c10
    Link-local IPv6 Address . . . . . : fe80::5062:d4cb:1d1a:d3f4712
    IPv4 Address. . . . . : 192.168.3.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.3.1

Tunnel adapter isatap.hsd1.ca.comcast.net.:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : hsd1.ca.comcast.net.

Tunnel adapter isatap.{57BF0931-F8A4-45A0-B4C1-34A646359608}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Tunnel adapter Local Area Connection* 11:

    Connection-specific DNS Suffix . . :
    IPv6 Address. . . . . : 2001:0:4137:9e74:2499:3213:3f57:fc9a
    Link-local IPv6 Address . . . . . : fe80::2499:3213:3f57:fc9a716
    Default Gateway . . . . . :

Tunnel adapter BT04 Adapter:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

C:\Users\patrickreg>

```

FIGURE 5.4 Using the ipconfig command.

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Fat>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Pat-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
DNS Proxy Enabled . . . . . : No
DNS Suffix Search List. . . . . : hsd1.ca.comcast.net.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . : hsd1.ca.comcast.net.
    Description . . . . . : Intel(R) PRO/1000 GT Desktop Adapter
    Physical Address. . . . . : 00-0E-0C-C3-06-16
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::9901:9fed:b646:3772x11(Preferred)
    IPv4 Address. . . . . : 192.168.3.181(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, November 07, 2009 5:26:31 PM
    Lease Expires . . . . . : Saturday, November 14, 2009 1:39:34 PM
    Default Gateway . . . . . : 192.168.3.1
    DHCP Server . . . . . : 192.168.3.1
    DHCPv6 IAID . . . . . : 234884620
    DHCPv6 Client DUID. . . . . : 00-01-00-01-12-7E-9C-D3-00-0E-0C-C3-06-16

    DNS Servers . . . . . : 4.2.2.2
    . . . . . : 68.87.76.182
    . . . . . : 68.87.76.134
    NetBIOS over Tcpip. . . . . : Enabled

```

FIGURE 5.5 Using the ipconfig /all command.

A typical troubleshooting process would be

1. Check local IP configuration (`ipconfig`).



2. Use the **ping** command to gather more information on the extent of the problem:
  - ▶ Ping the loopback address (127.0.0.1) or `::1`.
  - ▶ Ping the local IP address.
  - ▶ Ping the remote gateway.
  - ▶ Ping the remote computer.
3. Identify each hop (router) between two systems using the **tracert** command.
4. Verify DNS configuration using the **nslookup** command.

Using `ipconfig` with the `/all` switch shows you the IP configuration of the computer. If the IP address is invalid, communication might fail. If the subnet mask is incorrect, the computer has an incorrect Network ID and therefore communication might fail, especially to remote subnets. If the default gateway is incorrect or missing, the computer is not able to communicate with remote subnets. If the DNS server is incorrect or missing, the computer might not be able to resolve names and communication might fail.

If the computer is set to accept a DHCP server and one does respond, the computer uses Automatic Private IP Addressing (APIPA), which generates an IP address in the form of 169.254.xxx.xxx and the subnet mask of 255.255.0.0. After the computer generates the address, it broadcasts this address until it can find a DHCP server. When you have an Automatic Private IP Address, you can only communicate with computers on the same network/subnet that has an Automatic Private IP Address.

If you can successfully ping an IP address but not the name, name resolution is failing. If you successfully ping the computer name but the response does not resolve the FQDN name, resolution has not used DNS. This means a process such as broadcasts or WINS has been used to resolve the name, and applications that require DNS might fail. If you encounter a Request Timed Out message, this indicates that there is a known route to the destination computer but one or more computers or routers along the path, including the source and destination, are not configured correctly. A Destination Host Unreachable message indicates that the system cannot find a route to the destination system and therefore does not know where to send the packet on the next hop.

---

## Cram Quiz

1. What command would you use to release the IPv6 address handed out by a DHCP server?
  - A. `ipconfig /all`
  - B. `ipconfig /release`
  - C. `ipconfig /release6`
  - D. `ipconfig /flushdns`
2. What command can you use to query a DNS server for a name translation to an IP address?
  - A. `ipconfig`
  - B. `ipconfig /flushdns`
  - C. `ipconfig /registerdns`
  - D. `nslookup`

## Cram Quiz Answers

1. **C** is correct. The `ipconfig /release6` command releases the IPv6 address configured by a DHCP server. Answer A is incorrect because the `ipconfig /all` command only displays the IP configuration. Answer B is incorrect because the `ipconfig /release` command releases IPv4 addresses. Answer D is incorrect because the `ipconfig /flushdns` clears out the local DNS cache on a Windows system.
  2. **D** is correct. The `nslookup` command displays information that you can use to diagnose your DNS infrastructure. Answer A is incorrect because the `ipconfig` command only displays IP configuration. Answer B is incorrect because the `ipconfig /flushdns` command clears out the local DNS cache on a Windows system. Answer C is incorrect because the `ipconfig /registerdns` registers a system with a DNS server.
-

# Review Questions

1. What command would you use to renew the DHCP IPv4 addresses?
  - A. `ipconfig`
  - B. `ipconfig /renew`
  - C. `ipconfig /renew6`
  - D. `ipconfig /release_and_renew`
  - E. `ipconfig /registerdns`
2. What command would you use to flush the DNS cache stored on an individual Windows 7 machine?
  - A. `ipconfig`
  - B. `ipconfig /renew`
  - C. `ipconfig /renew6`
  - D. `ipconfig /registerdns`
  - E. `ipconfig /flushdns`
3. What command can be used to show network connectivity to a computer?
  - A. `ipconfig`
  - B. `arp`
  - C. `ping`
  - D. `tracert`
4. If you want to show IP addresses and their corresponding MAC addresses, what command would you use?
  - A. `ipconfig`
  - B. `ipconfig /all`
  - C. `arp`
  - D. `ping`
  - E. `tracert`
5. You are trying to figure out why a computer cannot connect to a file server. You type in `ipconfig` and you get the following output:

```
C:\Users\User>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : acme.com.
    Link-local IPv6 Address . . . . . : fe80::35d3:1958:365b:380a%13
    IPv4 Address. . . . . : 169.254.3.103
```

```
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

What is the problem?

- A. The computer cannot connect to the DHCP server to get an address.
  - B. The server was not assigned a default gateway.
  - C. The subnet mask is wrong.
  - D. You cannot determine the problem from this example.
6. You can ping a PC using an address but not by name. What is the problem?
- A. You are not on the same subnet as the computer.
  - B. A firewall is blocking access to the computer by name.
  - C. You need to start the DHCP client service on your PC.
  - D. You have a DNS name resolution problem.
7. You work as the desktop support technician at Acme.com. You want to assign an address to a computer that will be available on the Internet and it will have the same address for both IPv4 and IPv6. What kind of address is this?
- A. A unique private address
  - B. A multicast local address
  - C. A site-local address
  - D. A global unicast address
8. You work as the desktop support technician at Acme.com. You have a user that works between the Sacramento and New York offices. She currently has a static IP addresses assigned to her computer. When she is at the Sacramento office, her system has no problem connecting to the network. When she travels to New York, her system cannot connect to the network. What is the problem?
- A. You need to update the drivers for the network card.
  - B. You need to assign a Public IPv4 address.
  - C. You need to run the troubleshooting wizard.
  - D. Within the TCP/IPv4 Properties dialog box, you need to select the Obtain an IP address automatically option.
9. You are assigned a computer to test the IPv6 address of Server01. What command would you use?
- A. `ping -s server01`
  - B. `ping -6 server01`
  - C. `ping -a server01`
  - D. `ping -t server01`

10. Which type of IPv6 address is automatically configured and is used to communicate with local network devices such as a neighboring router?
- A. Global unicast address
  - B. Unique local unicast address
  - C. Link-local address
  - D. Anycast address

## Review Question Answers

1. Answer **B** is correct. To renew IPv4, you have to use the `ipconfig /renew` command. Answer A is incorrect because the `ipconfig` command without any options only displays basic IP configuration information. Answer C is incorrect because the `/renew6` option renews IPv6 IP addresses. Answer D is incorrect because the `/release_and_renew` option does not exist. Answer E is incorrect because the `/registerdns` option is how to get the computer to register itself with the DNS server.
2. Answer **E** is correct. The command to flush local cached DNS information is `ipconfig /flushdns`. Answer A is incorrect because the `ipconfig` command without any options only displays basic IP configuration information. Answer B is incorrect because the `/renew` option renews the IPv4 IP addresses. Answer C is incorrect because the `/renew6` option renews IPv6 IP addresses. Answer D is incorrect because the `/registerdns` option is how to get the computer to register itself with the DNS server.
3. Answer **C** is correct. The two commands that show network connectivity to another computer are the `ping` command and the `tracert` command. Answer A is incorrect because the `ipconfig` command without any options only displays basic IP configuration information. Answer B is incorrect because the `arp` command is used to view and manage IP address to MAC address mappings. The `tracert` command is found on UNIX and Linux machines. Windows machines use **tracert**.
4. Answer **B** is correct. To show all IP configuration information, you must use the `ipconfig /all` command. Answer A is incorrect because the `ipconfig` command without any options only displays basic IP configuration information. Answer C is incorrect because the `arp` command is used to view and manage IP address. Answers D and E are incorrect because `ping` and `tracert` are commands used to test network connectivity.
5. Answer **A** is correct. By looking at the example, the address assigned to the computer is 169.254.3.103, which is an Automatic Private IP address. Automatic Private IP addresses begin with 169.254. Automatic Private IP addresses are assigned to Windows computers when they cannot find a DHCP server from which to get an address. Answer B is incorrect because although a gateway address might be needed to communicate with computers on another network, the gateway was not assigned because it could not find a DHCP server. Answer

C is incorrect because this subnet mask was assigned when it could not find a DHCP server. Answer D is incorrect because you can determine the problem from the information provided in the example.

6. Answer **D** is correct. If you have a name resolution issue, the problem has to be with a DNS or WINS server or you have incorrect entries in your HOSTS or LMHOSTS files. Answer A is incorrect because if you can ping it by address, you have network connectivity to the server. So, it does not matter if the server is on the same subnet or a different subnet. Answer B is incorrect because you cannot block access to a computer by name but keep access by address. Answer C is incorrect because if the DHCP client service was not on, you would not be able to get any address from a DHCP server and are not able to connect to other hosts on the network.
7. Answer **D** is correct. If you want an address to be available from the Internet and be the same address for both IPv4 and IPv6, it must have a global unicast address that can be seen on the Internet. Answer A is incorrect because private addresses cannot be used on the public network such as the Internet. Answer B is incorrect because it has to be a single address assigned to a single computer, and not a multicast, which is used to broadcast to multiple addresses at the same time. Answer C is incorrect because a local address cannot be seen on the outside.
8. Answer **D** is correct. Because this person is traveling between two sites, the user needs to have a local address on each site. Therefore, you should let the local DHCP server hand out the addresses when she connects to each network. Answer A is incorrect because she can connect to one network. Therefore, the driver is working fine. Answer B is incorrect because this means that you are putting this computer directly on the Internet. Answer C is incorrect because running a troubleshooting wizard could be a lengthy process when the solution is simple.
9. Answer **B** is correct. To force the ping command to test a IPv6 connection, you need to use the `-6` option. Answer A is incorrect because the `-s` option is used to specify a source address, which can come in handy when you have a computer with multiple network cards. Answer C is incorrect because the `-a` option is used to resolve the address to a host name. Answer D is incorrect because the `-t` option pings the specified host until it is stopped.
10. Answer **C** is correct. Link-local addresses are used by hosts when communicating with neighboring hosts on the same link. Answer A is incorrect because a global unicast address is an address that is equivalent to IPv4 public addresses so they are globally routable and reachable on the IPv6 portion of the Internet. Answer B is incorrect because a unique local unicast address is an IPv6 address that is equivalent to IPv4 private address spaces. Answer D is incorrect because the anycast address is an IPv6 unicast address that is assigned to multiple computers. When IPv6 addresses communication to an anycast address, only the closest host responds.

*This page intentionally left blank*

## CHAPTER 6

# Configuring Advanced Windows Networking

**This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Network Connectivity:
  - ▶ Configure networking settings
- ▶ Configuring Mobile Computing:
  - ▶ Configure remote connections
  - ▶ Configure DirectAccess

Chapter 5, “Configuring Windows Networking,” covered the basics of networking including how to configure your computer to connect to a TCP/IP network. This chapter continues the discussion by looking at different networking technologies that you need to configure to connect to a network, which might include a wireless connection, a dial-up connection, or a VPN connection.



# Wireless Connection

## ► Configure networking settings

### CramSaver

1. You have a wireless access point configured to use Advanced Encryption Standard (AES) security; however, you do not have a pre-shared key. Which option should you use to connect to the wireless access point?
  - A. Use WPA2-Enterprise
  - B. Use WPA2-Personal
  - C. Use WPA-Enterprise
  - D. Use WPA-Personal
2. You have a laptop that runs Windows 7. At your corporation, the network administrators recently disabled the SSID broadcast. When you try to connect to the wireless network, you fail to connect. What do you need to do?
  - A. Change the wireless network connection settings on your computer
  - B. Update your Windows credentials
  - C. Enable network discovery
  - D. Install a digital certificate on the laptop

### Answers

1. **A** is correct. WPA2 uses AES encryption. Enterprise uses digital certificates instead of a pre-shared key. Answers B and D are incorrect because WPA and WPA2 Personal use a pre-shared key. Answer C is incorrect because WPA-Enterprise uses Temporary Key Integrity Protocol (TKIP) instead of AES.
2. **A** is correct. Because the SSID broadcast is disabled, the wireless network does not show up under the available networks list. Therefore, you need to manually configure the wireless connection. Answer B is incorrect because your Windows credentials are not used to connect to a wireless network. Answer C is incorrect because network discovery only helps you locate other wireless hosts on your wireless network. Answer D is incorrect because the digital certificate is needed to connect using WPA-Enterprise or WPA2-Enterprise; however, because you were able to connect to the network before and the only thing that has changed is that the SSID has been disabled, you most likely already have the appropriate digital certificate if necessary.

A quickly advancing field in networking is wireless technology. Today's computers can have a wireless network adapter to connect to other computers or to a wireless access point, which in turn enables the users to connect to the Internet or the rest of the internal network. Today's wireless adapters include PC cards for notebooks, Peripheral Component Interconnect (PCI)/PCI Express (PCIe) cards for desktops, and universal serial bus (USB) devices (which can be used with laptops or desktops).

Wireless adapters can run in one of two operating modes:

- ▶ **Ad hoc:** Wireless adapter used to connect directly to other computers with wireless adapters.
- ▶ **Infrastructure:** Wireless adapter connected to a wireless access point.

The most widely used wireless network adapters and access points are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specifications, as shown in Table 6.1. Most wireless networks used by companies are 802.11b, 802.11g, or 802.11n networks. Wireless devices that are based on these specifications can be Wi-Fi Certified to show they have been thoroughly tested for performance and compatibility.

### Note

Because these devices use common public low-powered wireless frequencies, other wireless devices such as wireless phones or handsets might interfere with wireless adapters if they use the same frequency when they are used at the same time.

TABLE 6.1 **Popular Wireless Standards**

Wireless Standard	802.11a	802.11b	802.11g	802.11n
Speed	Up to 54 Mbps	Up to 11 Mbps	Up to 54 Mbps	Up to 240 Mbps
Transmission frequency	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Effective indoor range	Approximately 25 to 75 feet	Approximately 100 to 150 feet	Approximately 100 to 150 feet	Approximately 300 to 450 feet
Compatibility	Incompatible with 802.11b and 802.11g.	802.11b wireless devices can interoperate with 802.11g devices (at 11 Mbps).	802.11g wireless devices can operate with 802.11b devices (at 11 Mbps).	802.11n can interoperate with 802.11b and 802.11g devices.

Of course, because a wireless network signal can be captured by anyone within the range of the antennas, it is easy for someone to intercept the wireless signals that are being broadcasted; therefore, it is always recommended that you use some form of encryption.

The most basic wireless encryption scheme is Wireless Equivalent Privacy (WEP). With WEP, you encrypt data using 40-bit, 128-bit, 152-bit, or higher private key encryption. With WEP, all data is encrypted using a symmetric key derived from the WEP key or password before it is transmitted, and any computer that wants to read the data must be able to decrypt it using the key. However, it is easy for someone with a little knowledge or experience to break the shared key because it doesn't change automatically over time. Therefore, it is recommended to use a higher form of wireless encryption than WEP.

Today, it is recommended that you use Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access Version 2 (WPA2). WPA was adopted by the Wi-Fi Alliance as an interim standard prior to the ratification of 802.11i. WPA2 is based on the official 802.11i standard and is fully backward compatible with WPA. 802.11i is another substandard of 802.11 that specifies an encryption standard to be used with wireless networks.

WPA provides strong data encryption via Temporal Key Integrity Protocol (TKIP), and WPA2 provides enhanced data encryption via Advanced Encryption Standard (AES), which meets the Federal Information Processing Standard (FIPS) 140-2 requirement of some government agencies. To help prevent someone from hacking the key, WPA and WPA2 rotate the keys and change the way keys are derived.

WPA-compatible and WPA2-compatible devices can operate in one of the following modes:

- ▶ **Personal mode:** Provides authentication via a preshared key or password.
- ▶ **Enterprise mode:** Provides authentication using IEEE 802.1X and Extensible Authentication Protocol (EAP).

802.1X provides an authentication framework for wireless local area networks (LANs), allowing a user to be authenticated by a central authority such as a RADIUS server. EAP is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), which support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

**ExamAlert**

Be sure to know the difference between WPA and WPA2 and between Personal mode and Enterprise mode.

In personal mode, WPA or WPA2 uses a preshared encryption key rather than a changing encryption key. The preshared encryption key is programmed into the access point and all wireless devices, which is used as a starting point to mathematically generate session keys. The session keys are then changed regularly so that the same session key is never used twice. Because the key rotation is automatic, key management is handled in the background.

In WPA or WPA2 Enterprise mode, wireless devices have two sets of keys:

- ▶ Session keys, which are unique to each association between an access point and a wireless client. They are used to create a private virtual port between the access point and the client.
- ▶ Group keys, which are shared among all clients connected to the same access point.

Both sets of keys are generated dynamically and are rotated to help safeguard the integrity of keys over time. The encryption key could be supplied through a certificate or smart card.

## Configuring Wireless Networks

Any wireless access point broadcasting within range should be available to a computer with a wireless adapter. By default, Windows 7 is set to enable you to configure the network settings that should be used. This enables you to configure different authentication, encryption, and communication options as necessary.

If you haven't previously connected to a wireless network, you can create a connection for the network by completing the following steps:

1. Open the **Network and Sharing Center**.
2. Click **Connect to a Network**. Select the network to which you want to connect. If the SSID is not listed for your network because it is not broadcasting, you have to go back to the Network and Sharing Center and click **Manage wireless networks** to create a network profile.
3. If it asks for a network security key, type in the security key and click **OK**.

4. Use the Security Type selection list to select the type of security being used. The encryption type is then filled in automatically for you.

You can also create a new wireless connection when the wireless network is not available or is hidden by doing the following:

1. Open the Network and Sharing Center and click **Set up a new connection or network**. Then click **Manually connect to a wireless network**. Click the **Next** button.
2. In the window shown in Figure 6.1, specify the Network Name (SSID), Security type, Encryption type, and Security Key. Then specify if you want to start the connection automatically and if you want to connect even if the network is not broadcasting. Click the **Next** button.
3. Click the **Close** button.

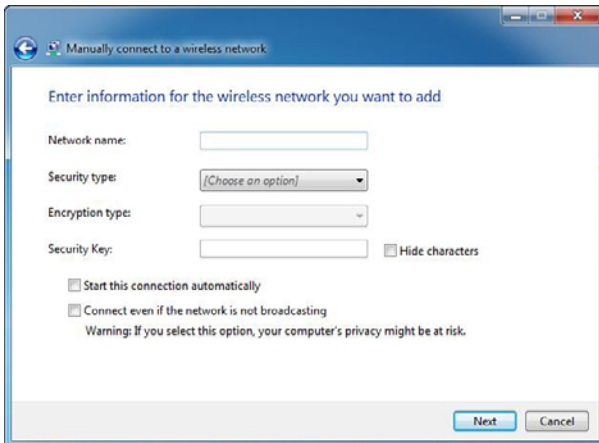


FIGURE 6.1 Manually connect to a wireless network.

To connect to a wireless or dial-up connection that you have defined, click the Network and Sharing Center icon in the Notification Area and click the connection to which you want to connect. If you move the mouse over a wireless network connection, you see the signal strength, security strength, radio type, and SSID (if available), as shown in Figure 6.2. You can also open the Network and Sharing Center and click **Connect** or **Disconnect** or click **Connect to a network**. To disconnect from a network connection, click the **Network and Sharing Center icon** in the Notification Area, click the connection from which you want to disconnect, and click the **Disconnect** button.

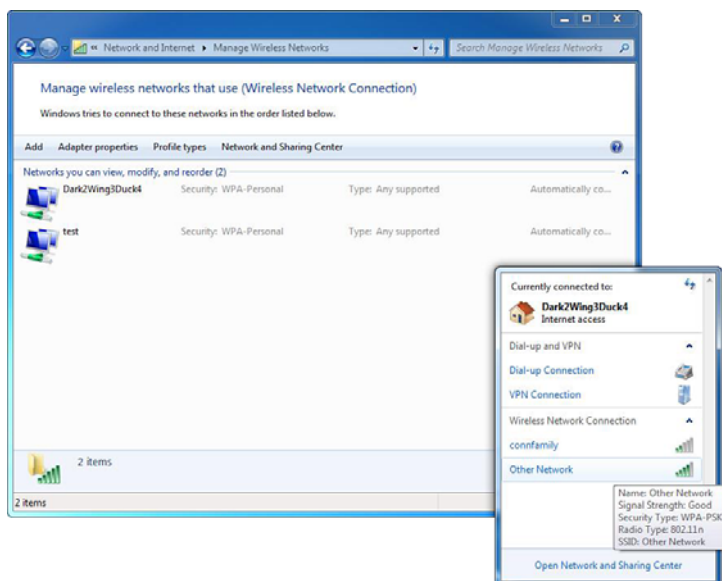


FIGURE 6.2 Displaying wireless connection characteristics.

If you open the Network and Sharing Center and double-click an active wireless network connection, you can view the status for the wireless connection including the duration, speed, and signal quality, as shown in Figure 6.3. You can also right-click a connection from the notification area and click **Status**.

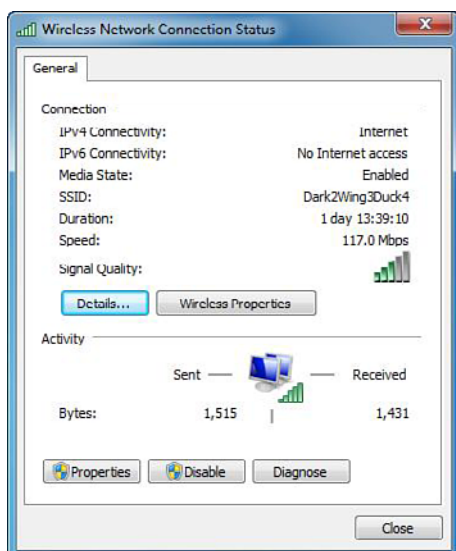


FIGURE 6.3 Wireless network connection status.

To manage all of your wireless network connections, just open the **Network and Sharing Center** and click **Manage wireless networks**. If you right-click an active connection and click **Properties** and view the **Connection** tab, as shown in Figure 6.4, you can specify how you connect to the wireless connection.

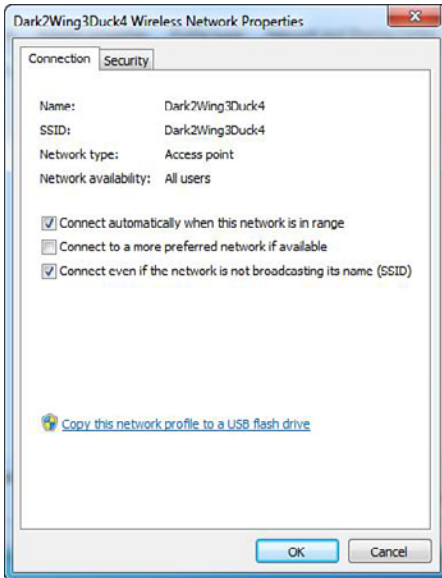


FIGURE 6.4 Connections options for a wireless connection.

If you select the **Security** tab, you can configure the **Security** type, **Encryption** type, and **Network security key**, as shown in Figure 6.5.

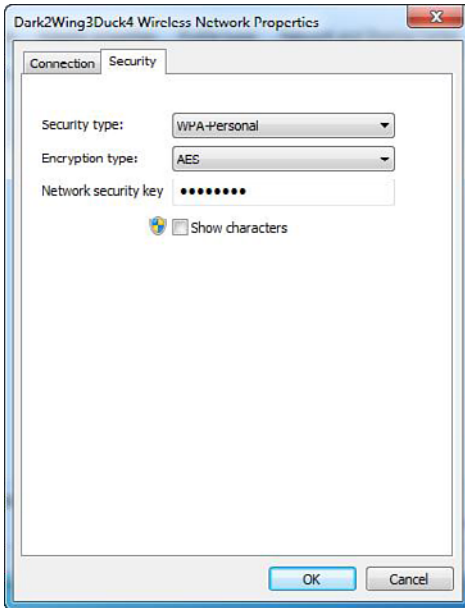


FIGURE 6.5 Security for a wireless connection.

If you have multiple computers that need to be configured to connect to a wireless network, you can use a USB flash drive to carry the configuration from computer to computer.

To save your wireless network settings to a USB flash drive, insert a USB flash drive into the computer, and then follow these steps:

1. Open the **Network and Sharing Center**.
2. In the left pane, click **Manage wireless networks**.
3. Right-click the network and then click **Properties**.
4. Click **Copy this network profile to a USB flash drive**. See Figure 6.6.
5. Select the USB device and then click **Next**. If you only have the one device, click the **Next** button. If you don't have a USB device connected, insert the USB device and click the **Next** button.
6. When the wizard is complete, click the **Close** button.



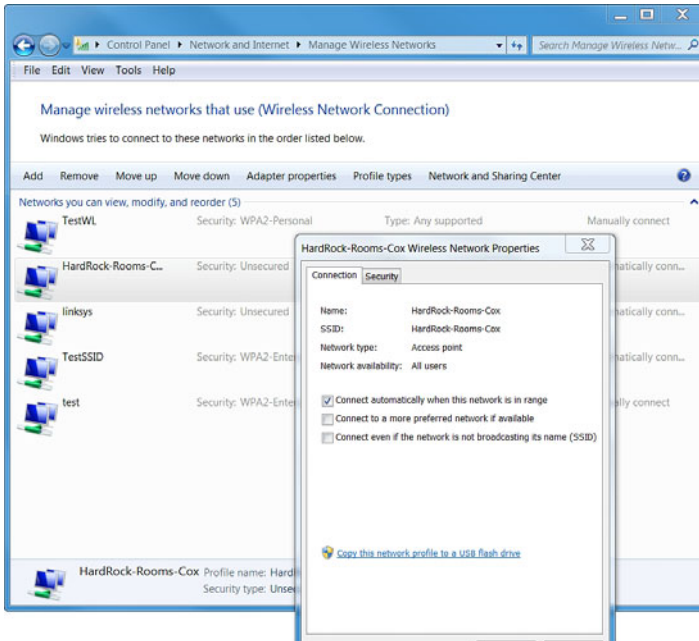


FIGURE 6.6 Copying a network profile to a USB flash drive.

To add a wireless computer running Windows 7 to a network by using a USB flash drive, do the following:

1. Plug the USB flash drive into a USB port on the computer.
2. For a computer running Windows 7, in the AutoPlay dialog box, click **Connect to a Wireless Network**.
3. When it asks if you want to add the network, click the **Yes** button.
4. When it says it was successful, click the **OK** button.

## Network Locations

The first time you connect to a network, you must choose a network location (sometimes known as a profile). This automatically sets the appropriate fire-wall and security settings for the type of network to which you connect. If you connect to networks in different locations, such as work, home, or your favorite coffee shop or hotel, choosing a network location can help ensure that your computer is always set to the appropriate security level.

There are four network locations:

- ▶ **Home network:** For home networks or when you know and trust the people and devices on the network. Network discovery is turned on for home networks, which enables you to see other computers and devices on the network and enables other network users to see your computer.
- ▶ **Work network:** For small office or other workplace networks. Network discovery is on by default, but you cannot create or join a homegroup.
- ▶ **Public network:** Used while you are visiting coffee shops, restaurants, hotels, and airports. This location is designed to keep your computer from being visible to other computers around you and to help protect your computer from any malicious software on the Internet. Homegroup is not available on public networks, and network discovery is turned off. It is recommended that you use this option when you are connected directly to the Internet without using a router, or if you have a mobile broadband connection.
- ▶ **Domain:** Used for domain networks such as those found in corporations. This type of network location is controlled by your network administrator and cannot be selected or changed.

To change a network location:

1. Click to open the **Network and Sharing Center**.
2. Click **Work network**, **Home network**, or **Public network**, as shown in Figure 6.7, and then click the network location you want.

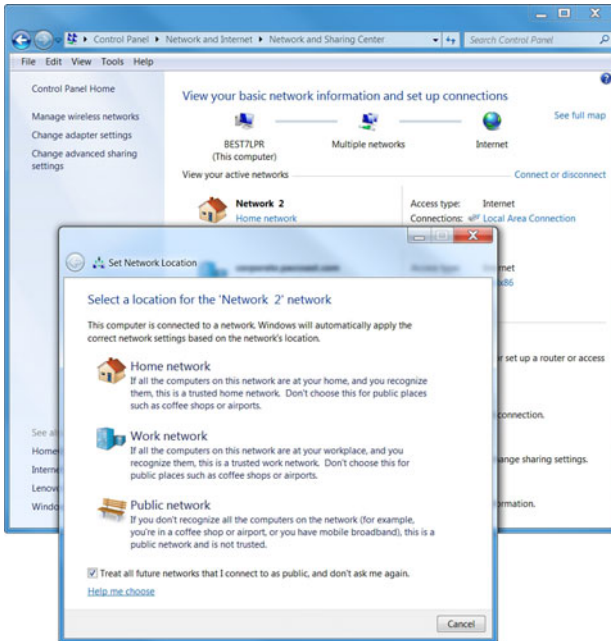


FIGURE 6.7 Setting network location.

---

## Cram Quiz

1. You have a wireless access point configured to use TKIP security with a pre-shared key. Which option should you use to connect to the wireless access point?
  - A. Use WPA2-Enterprise
  - B. Use WPA2-Personal
  - C. Use WPA-Enterprise
  - D. Use WPA-Personal
2. Your network administrator just installed a wireless access point for you to connect to. What do you need to do to connect to the wireless network?
  - A. Configure the Network Category of the wireless connection to Public
  - B. Configure the Network Category of the wireless connection to Private
  - C. Enable Internet Connection Sharing for your wireless network adapter
  - D. Configure the wireless network adapter to connect to the appropriate wireless network from the Connect to a network list

## Cram Quiz Answers

- D** is correct. WPA-Personal uses TKIP and uses a pre-shared key. Answers A and B are incorrect because WPA2-Enterprise and WPA2-Personal use AES encryption instead of TKIP. Answer C is incorrect because WPA-Enterprise uses a digital certificate instead of a pre-shared key.
  - D** is correct. To connect to a wireless network, you need to configure a connection to the wireless network. Assuming that SSID broadcast is enabled, you can then select the wireless network from the available network list. Just select the network and click Connect. Answer A is incorrect because setting it to public disables some network features such as network discovery, making your network connection more secure. Answer B is incorrect because making it Private opens up your network connection including enabling network discovery. In either case, public and private connections do not help you connect to the wireless network. Answer C is incorrect because enabling Internet Connection Sharing enables other people to use your computer to connect to the Internet. It does not help you connect to a wireless network.
-

# Remote Access

- ▶ **Configure remote connections**
- ▶ **Configure DirectAccess**

## CramSaver

1. You create a VPN connection for your corporate network. Where would you find the VPN connection when you want to connect remotely to your corporation?
  - A. Check Ease of Access
  - B. Check the Network and Sharing Center
  - C. Check in Mobile PC
  - D. Check the Parental Controls
  
2. How do you configure split-tunneling when using a VPN connection?
  - A. Right-click a VPN connection and click Properties. Then, under the Networking tab, open the Advanced options for the Internet Protocol 4 (TCP/IPv4). Lastly, deselect the Use default gateway on remote network option.
  - B. Right-click the VPN connection and click the Split-tunnel option.
  - C. Right-click the VPN connection and select Advanced options. Then select the Split-tunnel option.
  - D. Right-click the VPN connection and select Properties. Then select the Split-tunnel option.
  
3. What new technology introduced with Windows 7 provides a secure, always-on connection using IPsec and IPv6 that enables authorized users to access corporate shares, view intranet websites, and work with intranet applications without going through a traditional VPN?
  - A. BitLocker
  - B. DirectAccess
  - C. Teredo
  - D. ISATAP

## Answers

1. **B** is correct. The Network and Sharing Center is where you would go to view all your network connections, including VPN connections. Answer A is incorrect because Ease of Access is used to configure Windows 7 for disabled people. Answer C is incorrect because Mobile PC enables you to configure most common options necessary for laptop and other mobile computers. Answer D is incorrect because Parental Controls enables you to configure your computer to protect your children.
2. **A** is correct. To create a split tunnel, you need to right-click a VPN connection and click Properties. Then click the Networking tab and double-click the Internet Protocol Version 4 (TCP/IPv4) option. Click the Advanced button and deselect the Use default gateway on remote network. The other answers do not provide the correct instructions for creating a split tunnel.
3. **B** is correct. DirectAccess is a new technology that establishes a secure bi-directional connection to access a corporate network or resources. Answer A is incorrect because BitLocker is a full disk encryption tool introduced with Windows Vista and is included with Windows 7. Answers C and D are incorrect because Teredo and ISATAP are IPv6 technologies that help migrate from IPv4 to IPv6.

As a Windows 7 Technology Specialist, you might be expected to support users in remote locations including being at their homes. Remote connections connect individuals or groups to a network from a remote location. Windows 7 includes three types of remote connections:

- ▶ Dial-up
- ▶ Broadband
- ▶ Virtual private network (VPN)

## Dial-Up Connection

A dial-up connection is a nonpermanent point-to-point connection. Traditionally, it used a modem line and phone. A modem over a phone line is considered a legacy device network connection method with extremely slow bandwidth. In either case, you can open the **Network and Sharing Center** and click **Set up a new network or connect to a workplace**, as shown in Figure 6.8.

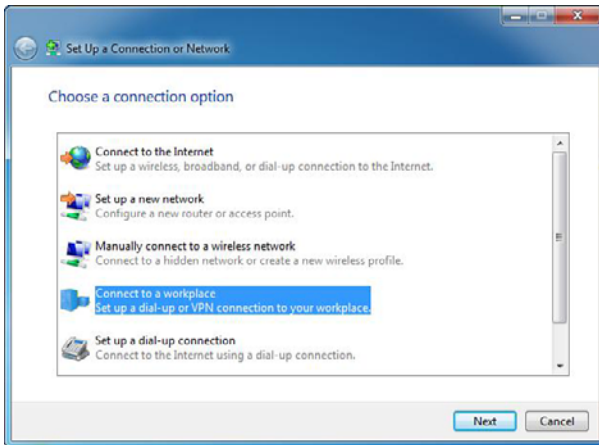


FIGURE 6.8 Setting up a connection or network.

Analog modems use dedicated telephone lines to connect users to the internal network at speeds up to 33.6 kilobits per second (Kbps). Digital modems use channels of an ISDN line to connect users to the internal network at speeds up to 56 Kbps. Communication is typically controlled by a Remote Access Server (RAS), which authenticates the login ID and password and authorizes the user to connect to the Internet or internal network.

If you are using a modem, you need to configure dialing rules so that the modem knows how the phone lines are accessed, what the caller's area code is, and what additional features should be used when dialing connections. Sets of dialing rules are saved as dialing locations in the Phone and Modem Options tool.

To view and set the default dialing location, follow these steps:

1. Click **Start** and then click **Control Panel**.
2. While in Icon view, double-click **Phone and Modem**.
3. The first time you start this tool, you see the Location Information dialog box.
4. Specify the country/region you are in, the area code (or city code), a number to access an outside line, and if the phone uses tone dialing or pulse dialing.

After you configure an initial location and click **OK**, you see the Phone and Modem Options dialog box.

To create a dial-up Internet connection to an ISP, follow these steps:

1. Open the **Network and Sharing Center**.
2. Click the **Set up a new connection or network** option.
3. If you already have an Internet connection, click the **Set up a new connection anyway** option.
4. Click **Dial-up**.
5. Set the phone number to dial for this connection, the user name, and password. You can also rename the connection name. If multiple people use the computer, you can select **Allow other people to use this connection**, as shown in Figure 6.9.
6. Click **Create**.

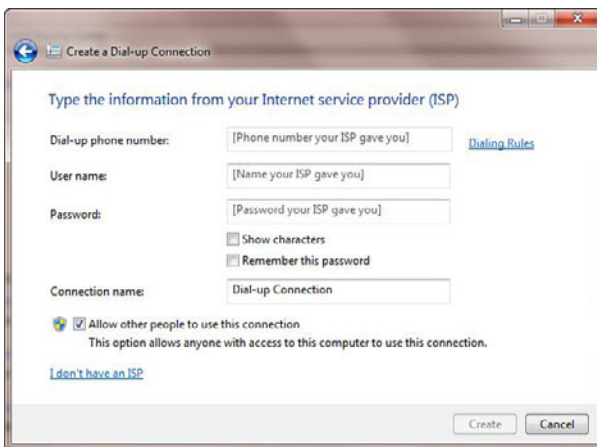


FIGURE 6.9 Create a Dial-up Connection dialog box.

After the connection has been defined, you can connect any time by opening the **Network and Sharing Center** and clicking **Connect to a network**.

You can also set up a connection to your computer from another computer by doing the following:

1. Open the **Control Panel**.
2. Click **Network and Internet**, click **Network and Sharing Center**, and then click **Manage Network Connections**.



**Note**

Some versions of Windows 7 accidentally labeled this link **Change adapter settings**.

3. Open the file menu and select **New Incoming Connection**.
4. Specify who can connect to a computer. If necessary, add someone. When complete, click the **Next** button.
5. From the window shown in Figure 6.10, choose to connect through the Internet or through a dial-up modem. Click the **Next** button.

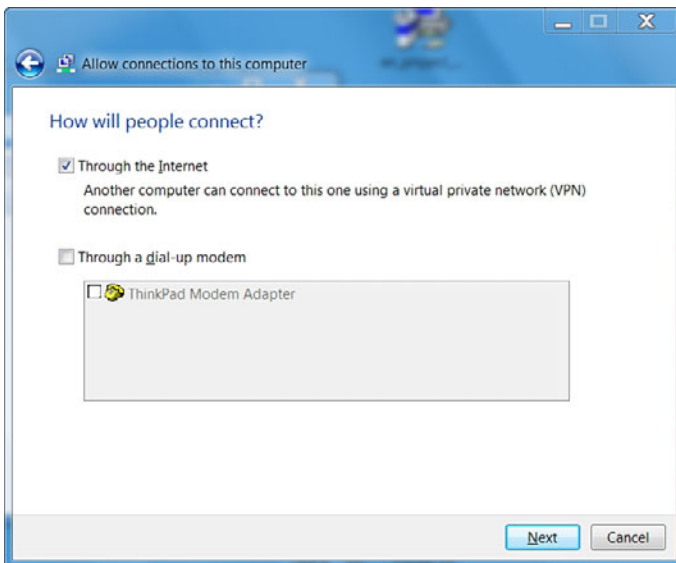


FIGURE 6.10 Specify how people will connect.

6. Select which network software you want available for the user and click **Allow access**, as shown in Figure 6.11.

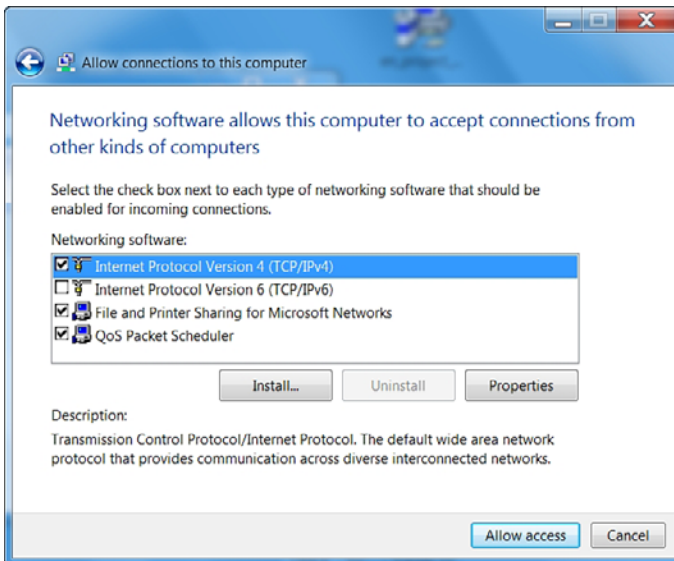


FIGURE 6.11 Allowing software to connect.

## Broadband Connection

Today, many connections are broadband connections, typically using a cable or DSL connection. Because these connections are always on, you don't need to set up dial-up rules or locations and you don't have to worry about ISP access numbers. Most broadband providers provide users with a router or modem, which users need to connect to the service provider. Most systems then use a network adapter on the computer to connect to a router or modem. In this configuration, the necessary connection is established over the LAN rather than a specific broadband connection. Therefore, it is the LAN that must be properly configured to gain access to the Internet. You won't need to create a broadband connection.

You can, however, create a specific broadband connection if needed. In some cases, you need to do this to set specific configuration options required by the ISP, such as secure authentication, or you might want to use this technique to set the user name and password required by the broadband provider. Although some ISPs might have you install their own software, other ISPs have you manually configure the broadband settings.

A common technology used for broadband is Point-to-Point Protocol over Ethernet (PPPoE). PPPoE is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. Today, it is typically found with DSL lines that require authentication. To configure a PPPoE connection, you do the following:

1. Open the **Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. Click **Connect to the Internet**.
4. Click **Broadband (PPPoE)**.
5. Specify a user name, password, and connection name and click the **Connect** button.

## Virtual Private Networking

A Virtual Private Network (VPN) is the creation of a secured, point-to-point connection across a private network or a public network such as the Internet. VPNs are used to establish secure communications channels over an existing dial-up or broadband connection. The data is encapsulated (data packets inserted into other data packets) before it is sent over the VPN connection. Because you send data on one end and it comes out the other end, it is often referred to as tunneling. In reality, a tunnel is logically defined where data is encrypted and sent embedded with data packets over a public network such as the Internet. Because the packets are encrypted, the data is unreadable by anyone who might get hold of the packets.

The VPN client authenticates to the remote access server, at which time they negotiate the tunneling and encryption technologies. Windows 7 supports the following VPN protocols:

- ▶ **Point-to-Point Tunneling Protocol (PPTP):** Based on PPP, which uses the Internet as a connection medium. Uses Microsoft Point-to-Point Encryption (MPPE) for 40-, 56-, and 128-bit encryption. PPTP is considered to have weak encryption and authentication; therefore, IPsec is usually preferred.
- ▶ **Layer 2 Tunneling Protocol (L2TP) with IP security (IPsec):** L2TP is the next-generation tunneling protocol based partially on PPTP. To provide encryption, L2TP uses IPsec. Because IPsec is considered a strong encryption, it is preferred over PPTP.

- ▶ **Secure Socket Tunneling Protocol (SSTP):** A tunneling protocol that uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the Secure Sockets Layer (SSL) channel of the HTTPS protocol. The use of PPP allows support for strong authentication methods, such as EAP-TLS. SSL provides transport-level security with enhanced key negotiation, encryption, and integrity checking.
- ▶ **Internet Key Exchange (IKEv2):** IKEv2 is a tunneling protocol that uses the IPsec Tunnel Mode protocol over UDP port 500. An IKEv2 VPN provides resilience to the VPN client when the client moves from one wireless hotspot to another or when it switches from a wireless to a wired connection. The use of IKEv2 and IPsec allows support for strong authentication and encryption methods.

### ExamAlert

If you don't want to open any additional ports on your firewall, you need to use SSTP.

When using VPNs, Windows 7 supports the following forms of authentication:

- ▶ **Password Authentication Protocol (PAP):** Uses plain text (unencrypted passwords). PAP is the least secure authentication.
- ▶ **Challenge Handshake Authentication Protocol (CHAP):** A challenge-response authentication that uses the industry standard MD5 hashing scheme to encrypt the response. CHAP was an industry standard for years and is still quite popular.
- ▶ **Microsoft CHAP version 2 (MS-CHAP v2):** Provides two-way authentication (mutual authentication). MS-CHAP v2 provides stronger security than CHAP.
- ▶ **EAP-MS-CHAPv2:** Extensible Authentication Protocol (EAP) is a universal authentication framework frequently used in wireless networks and Point-to-Point connections that allows third-party vendors to develop custom authentication schemes, including retinal scans, voice recognition, finger point identifications, smart card, Kerberos, and digital certificates. EAP-MS-CHAPv2 is a mutual authentication method that supports password-based user or computer authentication.

When configuring a VPN, you need to know the IP address or fully qualified domain name (FQDN) of the remote access server to which you are connecting. The steps for creating the VPN connection from a Windows 7 computer to a Windows Server 2008 computer are as follows:

1. From Control Panel, select **Network and Internet** to access the Network and Sharing Center.
2. From the Network and Sharing Center, choose **Set up a new connection or network Wizard**.
3. In Set Up a Connection or Network, choose **Connect to a workplace**.
4. In the Connect to a Workplace page, choose to **Use my Internet connection (VPN)**.
5. At the next screen, choose your VPN connection or specify the Internet Address for the VPN Server and a Destination Name. You can also specify the options to use a smart card for authentication, Allow other people to use this connection, and Don't connect now, just set up so I can connect later.

Often, you need to do additional configuration of your VPN connection, such as specifying the type of protocol, the authentication protocol to use, and the type of encryption, as shown in Figure 6.12 and Figure 6.13.

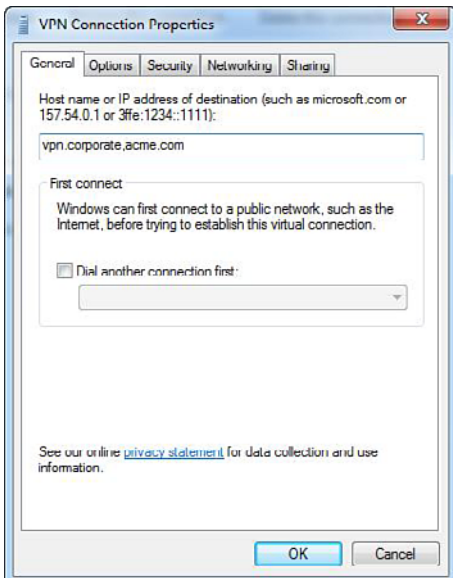


FIGURE 6.12 VPN Connection Properties: General tab.

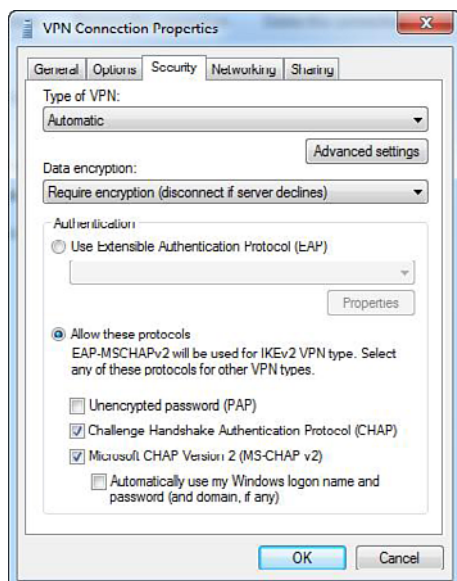


FIGURE 6.13 VPN Connection Properties: Security tab.

After the VPN connection is created and configured, to connect using the VPN, you just open the **Network and Sharing Center** and click **Change adapter settings**. Then right-click your VPN connection and click the **Connect** button.

## Split Tunneling

By default, the Use Default Gateway on the Remote Network option is enabled. As a result, a new default route is created on the VPN client. Data that cannot be sent to the local network is forwarded to the VPN connection. In other words, if you connect from home to your corporate network, all network traffic, including surfing the Internet, is routed through the VPN connection when you are connected through the VPN unless you need to talk to another computer on your home network. Having this option enabled helps protect the corporate network because all traffic also goes through firewalls and proxy servers, which helps prevent a network from being infected or compromised. When you disable the Use Default Gateway on Remote Network option, you are using a split tunnel. With the split tunnel, only traffic that is meant for your corporate network is sent through the default gateway on the remote network. When you want to surf the Internet, you use your local connection instead of the corporate network.

To enable split-tunnel:

1. Right-click a VPN connection and click **Properties**.
2. Click the **Networking** tab.
3. Double-click the **Internet Protocol Version 4 (TCP/IPv4)** option.
4. Click the **Advanced** button.
5. Deselect **Use default gateway on remote network**.

## DirectAccess

DirectAccess is a new feature in Windows 7 and Windows Server 2008 R2 that provides a secure, always-on connection that requires little or no user interaction using IPsec and IPv6. DirectAccess enables authorized users on Windows 7 computers to access corporate shares, view intranet websites, and work with intranet applications without going through a VPN. DirectAccess benefits IT professionals by enabling them to manage remote computers outside the office. Each time a remote computer connects to the Internet, before the user logs on, DirectAccess establishes a bi-directional connection that enables the client computer to remain current with company policies and to receive software updates.

Additional security and performance features of DirectAccess include the following:

- ▶ Support of multifactor authentication methods, such as a smart card for authentication.
- ▶ IPv6 to provide globally routable IP addresses for remote access clients.
- ▶ Encryption across the Internet using IPsec. Encryption methods include DES, which uses a 56-bit key, and 3DES, which uses three 56-bit keys.
- ▶ Integrates with Network Access Protection (NAP) to perform compliance checking on client computers before allowing them to connect to internal resources.
- ▶ Configures the DirectAccess server to restrict which servers, users, and individual applications are accessible.

**ExamAlert**

DirectAccess requires IPv6.

If your organization is not ready to fully deploy IPv6, IPv6 transition technologies such as ISATAP, 6to4, and Teredo enable clients to connect across the IPv4 Internet and to access IPv6 resources on the enterprise network.

DirectAccess helps reduce unnecessary traffic on the corporate network by sending traffic destined for the Internet through the DirectAccess server. DirectAccess clients can connect to internal resources by using one of the following methods:

- ▶ Selected server access
- ▶ Full enterprise network access

The connection method is configured using the DirectAccess console or it can be configured manually by using IPsec policies. For the highest security level, deploy IPv6 and IPsec throughout the organization, upgrade application servers to Windows Server 2008 R2, and enable selected server access. Alternatively, organizations can use full enterprise network access, where the IPsec session is established between the DirectAccess client and server.

DirectAccess clients use the following process to connect to intranet resources:

1. The DirectAccess client computer running Windows 7 detects that it is connected to a network.
2. The DirectAccess client computer attempts to connect to an intranet website that an administrator specified during DirectAccess configuration.
3. The DirectAccess client computer connects to the DirectAccess server using IPv6 and IPsec.
4. If a firewall or proxy server prevents the client computer using 6to4 or Teredo from connecting to the DirectAccess server, the client automatically attempts to connect using the IP-HTTPS protocol, which uses a Secure Sockets Layer (SSL) connection to ensure connectivity.
5. As part of establishing the IPsec session, the DirectAccess client and server authenticate each other using computer certificates for authentication.



6. By validating Active Directory group memberships, the DirectAccess server verifies that the computer and user are authorized to connect using DirectAccess.
7. If NAP is enabled and configured for health validation, the DirectAccess client obtains a health certificate from a Health Registration Authority (HRA) located on the Internet prior to connecting to the DirectAccess server.
8. The DirectAccess server begins forwarding traffic from the DirectAccess client to the intranet resources to which the user has been granted access.

To use DirectAccess, you need the following:

- ▶ One or more DirectAccess servers running Windows Server 2008 R2 with two network adapters
- ▶ At least one domain controller and DNS server running Windows Server 2008 or Windows Server 2008 R2
- ▶ A Public Key Infrastructure (PKI)
- ▶ IPsec policies
- ▶ IPv6 transition technologies available for use on the DirectAccess server

# Review Questions

1. You have laptop with an 802.11a wireless network card. When you boot the Windows 7 machine and you double-check the SSID, you cannot connect to your company's wireless network. What is the problem?
  - A. Your company is most likely using an 802.11b or 802.11g wireless network, with which 802.11a is incompatible.
  - B. The 802.11a network card is too slow, which is preventing a connection.
  - C. You need to change the SSID because it expired.
  - D. You need to assign an IP address to the wireless card.
2. You work as the desktop support technician at Acme.com. Your company just purchased 20 new laptops with wireless adapters. You have to configure each computer to connect to the network wirelessly with the least amount of administrative effort. What should you do?
  - A. Manually configure each computer's wireless adapter
  - B. Save the wireless network settings to a USB device and apply it to each computer
  - C. Copy the wireless network settings to a shared folder and access the configuration from each laptop
  - D. Copy the wireless network settings to the hard disk of each of the new computers
3. You work as the network administrator at Acme.com. Your company just purchased 20 new laptop computers, which are going to connect to the new wireless network. You want the computers to connect to the network using TKIP without requiring the use of any security key or pass phrase. Which option would you select in the wireless network dialog box?
  - A. The WEP option
  - B. The WPA-Personal
  - C. The WPA2-Personal
  - D. WPA-Enterprise
  - E. WPA2-Enterprise

4. You are a desktop support technician for Acme.com. You are configuring several new laptops with Microsoft Windows 7 Enterprise. You need to configure a connection so that the users can connect to the Acme.com internal network while working from home. What steps do you need to do to set this up?
- A. Open the Network and Sharing Center in Control Panel. Click Setup a new connection or network from the Task List. Choose Connect to a workplace under the Choose a connection option. Choose VPN under How do you want to connect. Enter the Internet address of the server to which you want to connect.
  - B. Click Manage Network connections from the Start menu. Click Setup connection or network from the Task List. Choose Connect to a workplace under the Choose a connection option. Choose Dial-up connection under How do you want to connect. Enter the Internet address of the server to which you want to connect.
  - C. Open the Network connections interface. Click Setup connection or network from the Task List. Choose Connect to a workplace under Choose a connection option. Enter the Internet address of the server to which you want to connect.
  - D. Open the Network and Sharing Center in Control Panel. Click Setup connection or network from the Task List. Choose Connect to a VPN under Choose a connection option. Choose Workplace under How do you want to connect. Enter the Internet address of the server to which you want to connect.
5. Your network administrator just installed a new wireless router to which you connect; however, you find out that you cannot discover other computers on the local wireless network. What should you do?
- A. Configure the wired and wireless network adapters as a network bridge
  - B. Change the network category settings of the wireless connection to public
  - C. Change the network category settings of the wireless connection to private
  - D. Disable the Windows firewall
6. You have a wireless network to which you connect, but the SSID broadcasts have been disabled. What should you do to connect to the wireless network?
- A. Click the Set up a connection or network link and select the Set up a wireless ad hoc network option
  - B. Click the Connect to network link and then right-click the appropriate network and select the Connect option

- C.** Click the View computers and devices link and then right-click the wireless access point (WAP) and select the Enable option
  - D.** Click the Set up a connection or network link and select the Manually connect to a wireless network option
- 7.** You have a computer with Windows 7. You create a VPN connection; however, you want to be able to connect to the VPN while making sure that Internet traffic does not go through the corporate network. What should you do?
- A.** Assign a static IP address and default gateway for the VPN connection
  - B.** Configure the security settings of the VPN connection
  - C.** Configure the Advanced TCP/IP settings of the VPN connection
  - D.** Configure a static DNS server for the VPN connection
- 8.** To protect a tunnel created with L2TP, what protocol should you use to provide encryption?
- A.** MPPE
  - B.** IPsec
  - C.** SSTP
  - D.** CHAP
- 9.** When using authentication, which of the following authentication methods is the least secure?
- A.** PAP
  - B.** CHAP
  - C.** MS-CHAPv2
  - D.** EAP-MS-CHAPv2
- 10.** DirectAccess requires which protocol to operate?
- A.** IPv4
  - B.** IPv6
  - C.** HTTPS
  - D.** PPTP

## Review Question Answers

1. Answer **A** is correct. In corporations today, most wireless networks use 802.11b, 802.11g, or 802.11n. Because 802.11a is not compatible with 802.11b/g, it is most likely the problem. Answer B is incorrect because the 802.11b and g can operate at lower speeds. Answer C is incorrect because although having the wrong SSID causes problems, the SSID does not expire. Answer D is incorrect because most networks have DHCP service to assign IP addresses.
2. Answer **B** is correct. You can save the information to a USB device and then use that device to copy the configuration to each computer. Answer A is incorrect because, although A works, it requires a lot more administrative effort. Answer C is incorrect because these computers do not have wired network cards to connect to a shared drive. Answer D is incorrect because copying the network settings also requires a lot more administrative effort because you need somehow get the setting to each hard drive.
3. Answer **D** is correct. WPA uses TKIP and WPA Enterprise does not require a security key or pass phrase. Instead a certificate or similar technology is used to provide the initial key. Answer A is incorrect because WEP does not use TKIP and requires a key to be supplied. Answer B is incorrect because Personal means that you have to enter a security key or pass phrase. Answers C and E are incorrect because they use AES instead of TKIP.
4. Answer **A** is correct. To connect to the office over the Internet you need to set up a VPN connection. The correct order to set up a VPN connection is the following:
  1. Open the **Network and Sharing Center** in Control Panel. This is the interface in Windows 7 that enables you to view, set up, and troubleshoot network connections as well as enable sharing on your computer.
  2. Click **Set up a connection or network** from the Tasks list. This is the option that enables you to create new connections, such as dial-up, wireless, or VPN connections.
  3. Under the **Choose a connection** option, choose **Connect to a workplace**. This is the section that enables you to set up VPN connections. The other options, such as Set up a dial-up connection, do not allow you to connect to an office over the Internet.
  4. Under **How do you want to connect**, choose **VPN**. A VPN connection enables you to tunnel over the Internet to a VPN server at the office.
  5. Enter the Internet address of the server to which you want to connect. To connect to a VPN server, you need to provide a name and IP address for the connection.

Answer **B** is incorrect because you do not click Manage Network Connections from the Start menu. Answer C is incorrect because to set up a VPN, you do not open a network connections interface. Answer D is incorrect because you do not choose Connect to a VPN; instead, you first choose Connect to a workplace.

5. Answer **C** is correct. If the network category is set to public (Answer B), network discovery is disabled. Therefore, you need to change it from public to private. Answer A is incorrect because a bridge enables communications between a wired and wireless network through your computer. Answer D is incorrect because enabling or disabling the Windows firewall would not enable the network discovery feature.
6. Answer **D** is correct. If the wireless access point is configured not to broadcast, you need to configure your wireless connection manually. Answer A is incorrect because you use Ad hoc network options when you want to connect to fellow wireless hosts without using a wireless router. Answer B is incorrect because the network SSID is not broadcasted, so it does not show up on the list; therefore, you cannot right-click the connection. Answer C is incorrect because you are not be able see the wireless access point because the SSID broadcast is disabled, not the WAP itself.
7. Answer **C** is correct. By default, when connected through a VPN, all traffic goes through the default gateway on the remote network. If want to use your own local connection to surf the Internet, you need to enable split tunneling by configuring the Advanced TCP/IP settings and disabling the Use Default Gateway on the Remote Network option. Answer A is incorrect because assigning a static IP address and default gateway does not create a split tunnel. Answer B is incorrect because there is no security setting to create a split tunnel. Answer D is incorrect because using a static DNS server does not create a split tunnel.
8. Answer **B** is correct. To provide security for L2TP, you use IPsec. Answer A is incorrect because MPPE is the encryption used for PPTP. SSTP uses HTTPS protocol that uses SSL to encrypt data. Therefore, Answer C is incorrect. Answer D is incorrect because CHAP is an authentication protocol and is not used to encrypt the data.
9. Answer **A** is correct. PAP, short for Password Authentication Protocol, sends the password in plain text (unencrypted password). Answers B, C, and D use some form of encryption when dealing with passwords. Therefore, CHAP, MS-CHAPv2, and EAP-MS-CHAPv2 are all more secure than PAP.
10. Answer **B** is correct. DirectAccess is a new feature in Windows 7 and Windows Server 2008 R2 that provides a secure, always-on connection that requires little or no user interaction using IPsec and IPv6. Answers A, C, and D are incorrect because DirectAccess does not use IPv4, HTTPS, or PPTP.

*This page intentionally left blank*

## CHAPTER 7

# Configuring Windows Firewall and Windows Defender

**This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Network Connectivity
- ▶ Configure Windows Firewall

In today's world, there is often a need for users to share data with other users. This chapter focuses on sharing files so those users can access files from a Windows 7 computer over the network and how to control such access so that it remains secure.



# Spyware and Windows Defender

## ► Configure Windows Firewall

### CramSaver

1. What would you use to help protect against spyware when surfing the Internet?
  - A. CHKDSK
  - B. Scandisk
  - C. Windows Defender
  - D. IPsec
2. You work as the desktop support technician at Acme.com. You want to use the fastest scan that checks the most common locations where spyware is normally found. Which type of scan would you do?
  - A. Quick scan
  - B. Fast scan
  - C. Full scan
  - D. Custom scan

### Answers

1. **C** is correct. To help protect against spyware, Microsoft includes two utilities. The first one specifically aimed at spyware is Windows Defender. The other utility is Windows Firewall. CHKDSK (Answer A) and Scandisk (Answer B) look for errors on the hard drive for older versions of Windows but do not protect against spyware. Scandisk has been replaced by Error-Checking. Answer D is incorrect because IPsec is a protocol used to secure packets sent between a source and a target.
2. **A** is correct. Quick scan checks all places that you normally find spyware, including those that execute during startup. Answer B is incorrect because a fast scan does not exist. Answer C is incorrect because full scans are much more thorough scans and take much longer. Answer D is incorrect because you need to manually specify where to search for spyware.

Spyware is a common threat to computers that can cause problems similar to a virus. Spyware (including adware) programs are malware that can be installed on computers, and they collect little bits of information at a time about a user without his or her knowledge. Some machines are infected with spyware when the spyware is bundled with other software, often without the user's knowledge. Sometimes spyware software might be added and the only notification the user gets is specified in the fine print of an End User License Agreement (EULA), which is usually a long document written with lots of legal jargon and is not read by most users. Spyware can also be picked up by simply visiting various websites because it is often hidden as ActiveX controls.

After it's installed, the spyware can monitor user activity on the Internet and transmit information such as email addresses, passwords, and credit card numbers without the user's knowledge. This information can be used for advertising or marketing purposes, to give the information to other parties, or to use the information for illegal purposes. Spyware can do the following:

- ▶ Generate annoying pop-ups
- ▶ Monitor keystrokes
- ▶ Scan files on the hard drive
- ▶ Snoop other applications such as chat programs or word processors
- ▶ Install other spyware programs
- ▶ Read cookies
- ▶ Change the default home page on a web browser to other links or default pages
- ▶ Open your computer to be accessed by others

### ExamAlert

It is important that you know the symptoms of spyware so when you are presented with a troubleshooting question, you know the appropriate steps to mitigate spyware issues.

Spyware can also use network bandwidth and computer memory and can lead to system crashes or general system instability.

To reduce your chances of being affected by spyware, you should

- ▶ Use a good antivirus package such as Norton AntiVirus, McAfee VirusScan, or Microsoft Security Essentials.

- ▶ Use spyware detection and removal programs such as Windows Defender if the detection/removal capabilities are not included in the antivirus software.
- ▶ Be sure that your machine has all security patches and fixes loaded.
- ▶ Install software only from sources and websites you trust.
- ▶ Be careful what software you install on your system. Be sure to read the EULA for any piece of shareware or file sharing package you plan on installing.
- ▶ Keep your web browser security settings at medium or higher.
- ▶ Install or enable a personal firewall such as Windows Firewall that is included with Windows 7.
- ▶ Use pop-up blockers.

Windows Defender, included with Windows 7, helps users detect and remove known spyware and other potential unwanted software. Windows Defender protects your computer with automated and real-time scanning and software removal.

Because spyware and other potentially unwanted software can try to install itself on your computer any time you connect to the Internet or when you install programs, it is recommended that you have Windows Defender running whenever you are using your computer.

Windows Defender offers three ways to help keep spyware and other potentially unwanted software from infecting your computer:

- ▶ **Real-time protection:** When it runs in the background, Windows Defender alerts you when spyware or potentially unwanted software attempts to install itself or to run on your computer. It also alerts you when programs attempt to change important Windows settings.
- ▶ **Scanning options:** You can use Windows Defender to actively scan your disks for spyware and other potentially unwanted software that might be installed on your computer and to automatically remove any malicious software that is detected during a scan as demonstrated in Figure 7.1. You can set up Windows Defender to scan automatically according to a schedule, or you can run it manually.
- ▶ **SpyNet community:** The online Microsoft SpyNet community helps you see how other people respond to software that has not yet been classified for risks.

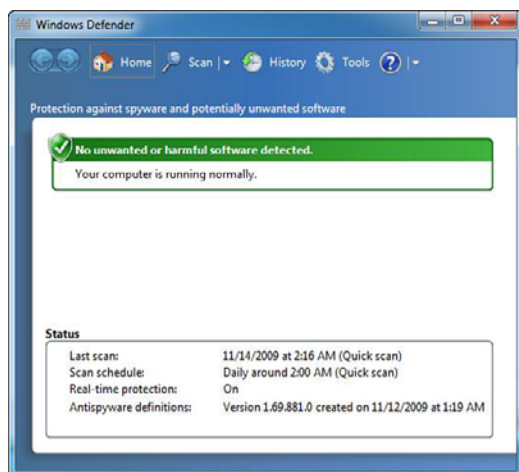


FIGURE 7.1 Windows Defender.

You can also use Windows Defender to constantly monitor your system, which offers your system real-time protection. The real-time protection uses nine security agents to monitor the critical areas of your computer that spyware might attack. When an agent detects potential spyware activity, it stops the activity and raises an alert. The agents include

- ▶ **Microsoft Internet Explorer Configuration:** Monitors browser security settings.
- ▶ **Internet Explorer Downloads:** Monitors applications that work with Internet Explorer, such as ActiveX controls and software installation applications.
- ▶ **Internet Explorer Add-ons (Browser Helper Objects):** Monitors applications that automatically run when you start Internet Explorer.
- ▶ **Auto Start:** Monitors the list of applications that starts when Windows starts.
- ▶ **System Configuration:** Monitors security-related settings in Windows.
- ▶ **Services and Drivers:** Monitors services and drivers as they interact with Windows and applications.
- ▶ **Windows Add-ons:** Monitors software utilities that integrate with Windows.
- ▶ **Application Execution:** Monitors applications when they start and throughout their execution.

- ▶ **Application Registration (API Hooks):** Monitors files and tools in the operating system where applications can insert themselves to run.

Windows Defender includes automatic scanning options to provide regular spyware scanning in addition to on-demand scanning options. The scan options include

- ▶ **Quick Scan:** A quick scan checks areas on a hard disk that spyware is most likely to infect.
- ▶ **Full Scan:** A full scan checks all critical areas, including all files, the registry, and all currently running applications.
- ▶ **Custom Scan:** A custom scan enables users to scan specific drives and folders.

#### Note

A quick scan checks locations where spyware is normally found.

When you perform a scan, you can configure what Windows Defender does when it identifies unwanted software, as shown in Figure 7.2. The actions include

- ▶ **Recommended action based on definition:** Windows Defender performs an action based on what is in the definition.
- ▶ **Quarantine:** Windows Defender places identified unwanted software in a quarantine or isolated holding folder. You can check the item before removing it from the system.
- ▶ **Remove:** Windows Defender removes the item from the system.
- ▶ **Allow:** Windows Defender does not take any action.

To prevent Windows Defender from automatically taking the recommended action, such as quarantining or removing software detected during a scan, you need to clear **Apply recommended actions** located at the bottom of the Options screen. As a result, Windows defender recommends an action to take for detected malicious software.

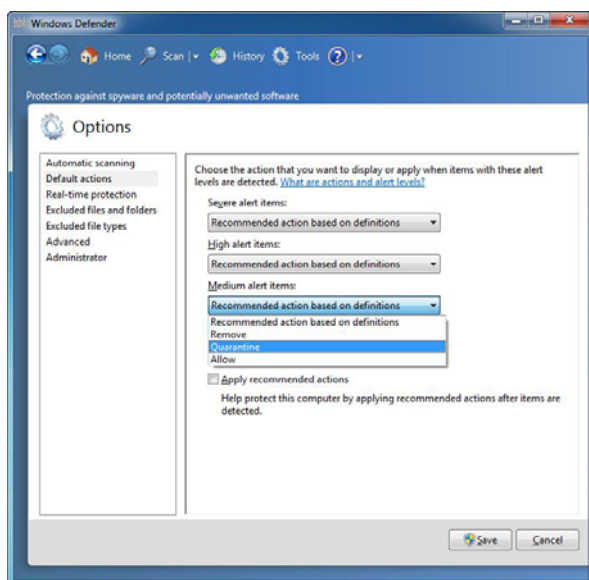


FIGURE 7.2 Configuring Windows Defender options.

Similar to antivirus software, Windows Defender uses a definition database that lists and details and characteristics of known spyware. Also similar to antivirus software, the definition database becomes out of date as new spyware is introduced. Therefore, you must update the database regularly for it to be effective.

To turn Windows Defender on or off, do the following:

1. Open **Windows Defender**, open a search box and type in **Windows Defender**, and press **Enter**.
2. Click **Tools** and then click **Options**.
3. Under Administrator options, select or clear the **Use this program** checkbox and then click **Save**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

To turn Windows Defender real-time protection on or off, follow these steps:

1. Open **Windows Defender**.
2. Click **Tools** and then click **Options**.
3. Under Real-time protection options, as shown in Figure 7.3, select the **Use real-time protection (recommended)** checkbox.

4. Select the options you want. To help protect your privacy and your computer, you should select all real-time protection options.
5. Under Choose if Windows Defender should notify you about, select the options you want and then click **Save**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

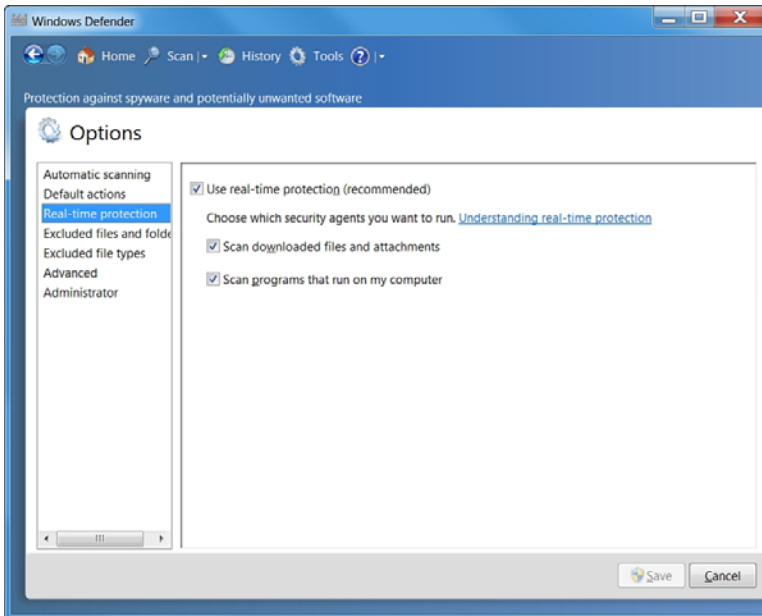


FIGURE 7.3 Configuring Windows Defender real-time protection.

If you trust software that Windows Defender has detected, you can stop Windows Defender from alerting you to risks that the software might pose to your privacy or your computer. To stop being alerted, you need to add the software to the Windows Defender allowed list. If you decide that you want to monitor the software again later, you can remove it from the Windows Defender allowed list at any time.

To add an item to the allowed list, the next time Windows Defender alerts you about the software, click **Always Allow** on the Action menu in the Alert dialog box. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

To remove an item from the allowed list, do the following:

1. Open **Windows Defender**.

2. Click **Tools** and then click **Allowed items**.
3. Select the item that you want to monitor again, and then click **Remove from List**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

---

## Cram Quiz

1. What do you call a type of malware that can monitor user activity on the Internet and transmit information such as email addresses, passwords, and credit card numbers without the user's knowledge?
  - A. Spyware
  - B. Worm
  - C. Cookies
  - D. EULA
2. When you find unwanted software, what do you call it when the unwanted software is placed in an isolated holding folder?
  - A. Quick scan
  - B. Quarantine
  - C. Recycle Bin
  - D. Cookie

## Cram Quiz Answers

1. **A** is correct. Spyware is a common threat to computers that can cause problems similar to a virus. Some of the symptoms include generating annoying pop-ups, monitoring keystrokes, scanning files on hard drives, and transmitting confidential information. Answer B is incorrect because a worm is a form of malware that replicates and consumes valuable resources including bandwidth. Answer C is incorrect because a cookie is a text file used to remember settings when visiting a website. Answer D is incorrect because a EULA is the End User License Agreement.
  2. **B** is correct. You can have Windows Defender place possible unwanted software into a quarantine folder so that it can be reviewed to determine if it is malware. Answer A is incorrect because a quick scan is a type of scan that is used by Windows Defender to verify key areas where spyware is most likely found. Answer C is incorrect because the Recycle Bin is a temporary holding area where deleted objects are stored. Answer D is incorrect because a cookie is a text file used to remember settings when visiting a website.
-



# Windows Firewall

## ► Configure Windows Firewall

### CramSaver

1. Which network location used with Windows Firewall is more secure by disabling network discovery and homegroups?
  - A. Home network
  - B. Work network
  - C. Public network
  - D. Domain
2. Anytime you are having problems accessing a common network program or application and you cannot connect, what should you check?
  - A. Windows Defender
  - B. Your antivirus program
  - C. Windows Firewall
  - D. IPsec

### Answers

1. **C** is correct. The public network location is designed to keep your computer from being visible to other computers around you and to help protect your computer from any malicious software on the Internet. A homegroup is not available on public networks, and network discovery is turned off. Answer A is incorrect because it is designed for home networks or when you know and trust the people and devices on the network. Network discovery is turned on for home networks. Answer B is incorrect because work network is for small office or other workplace networks. Network discovery is on by default, but you cannot create or join a homegroup when using the work network location. Answer D is incorrect because the domain network is used for domain networks found in corporations.
2. **C** is correct. Windows firewall is a packet filter and stateful host-based firewall that allows or blocks network traffic according to the configuration. You should check Windows Firewall to see if it is blocking you from accessing the network program or application. Answer A is incorrect because Windows Defender is used to protect a computer against spyware. Answer B is incorrect because although some antivirus programs have firewall capability, it is most likely the Windows Firewall that is blocking the program. Answer D is incorrect because IPsec is used to encrypt network traffic.

Because most computers are connected to the Internet through dialup, broadband (such as DSL or cable modems), or a local area network (LAN), computers are vulnerable to attack or unauthorized access. To help protect your system, you should have a firewall between you and the outside world. The firewall monitors all traffic coming in and going out to prevent unauthorized access.

Windows Firewall is a packet filter and stateful host-based firewall that allows or blocks network traffic according to the configuration. A packet filter protects the computer by using an access control list (ACL), which specifies which packets are allowed through the firewall based on IP address and protocol (specifically the port number). A stateful firewall monitors the state of active connections and uses the information gained to determine which network packets are allowed through the firewall. Typically, if the user starts communicating with an outside computer, it remembers the conversation and allows the appropriate packets back in. If an outside computer tries to start communicating with a computer protected by a stateful firewall, those packets are automatically dropped unless granted by the ACL.

### ExamAlert

Remember that any program or service that needs to communicate on a network, including sharing files, must be opened in a firewall.

### Note

Although Windows has a built-in software firewall, it is only one component used to protect your computer. If you have a home network, you should use a router that has a built-in firewall to help protect your network and your computers when the network is connected to the Internet. Organizations that have Internet connections should have a solution that includes one or more enterprise firewalls.

Firewall rules that can be defined include

- ▶ **Inbound rules:** These rules help protect your computer from other computers making unsolicited connections to it.
- ▶ **Outbound rules:** These rules help protect your computer by preventing your computer from making unsolicited connections to other computers.
- ▶ **Connection-specific rules:** These rules enable a computer's administrator to create and apply custom rules based on a specific connection.

## Basic Configuration

Windows Firewall is on by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, you can add it to the Exceptions list (on the Exceptions tab). For example, you might not be able to send photos in an instant message until you add the instant messaging program to the Exceptions list.

To turn on or off Windows Firewall:

1. Open Windows Firewall by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **Windows Firewall**.
2. In the left pane, click **Turn Windows Firewall on or off**, as shown in Figure 7.4. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Below each network location type, click **Turn on Windows Firewall**, and then click **OK**. It is recommended that you turn on the firewall for all network location types.

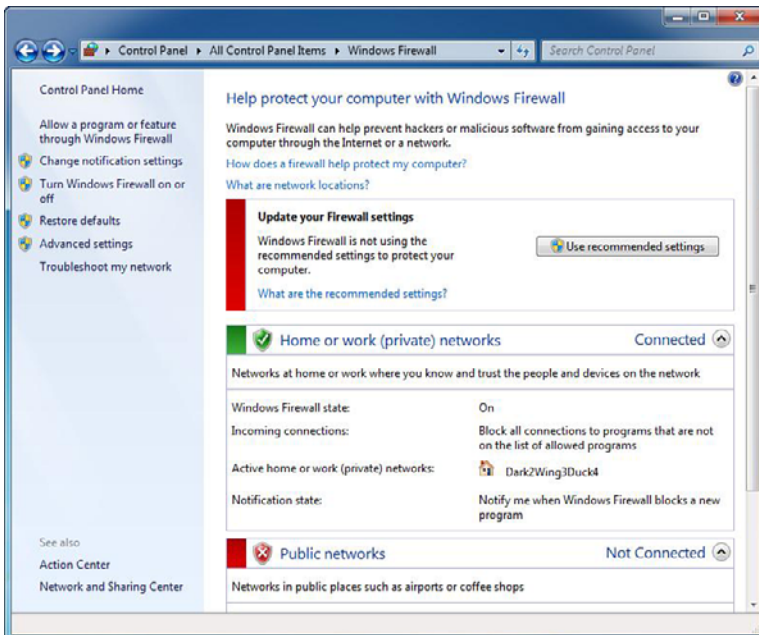


FIGURE 7.4 Windows Firewall.

Besides turning the firewall off and on for each profile, you also have the following options:

- ▶ **Block all incoming connections, including those in the list of allowed programs:** This setting blocks all unsolicited attempts to connect to your computer. Use this setting when you need maximum protection for your computer, such as when you connect to a public network in a hotel or airport, or when a known computer worm is spreading over the Internet. With this setting, you aren't notified when Windows Firewall blocks programs, and programs in the list of allowed programs are ignored. When you block all incoming connections, you can still view most web pages, send and receive email, and send and receive instant messages.
- ▶ **Notify me when Windows Firewall blocks a new program:** If you select this checkbox, Windows Firewall informs you when it blocks a new program and gives you the option of unblocking that program.

The first time you connect to a network, you must choose a network location (sometimes known as profiles). This automatically sets the appropriate firewall and security settings for the type of network that you connect to. If you connect to networks in different locations, such as work, home, or your favorite coffee shop or hotel, choosing a network location can help ensure that your computer is always set to the appropriate security level. See Figure 7.5.

### ExamAlert

You need to know the various network locations and when to use them so that your computer is protected as much as possible while allowing the access that you need.

Traditionally with firewalls, you can open or close a protocol port so that you can allow or block communication through the firewall. With the Windows Firewall included with Windows 7, you specify which program or feature you want to communicate through the firewall. The most common options are available by clicking the **Allow a program or feature through Windows Firewall** option, as shown in Figure 7.6. If you need to open a port instead of specifying a program, you have to use the Windows Firewall with Advanced Security.

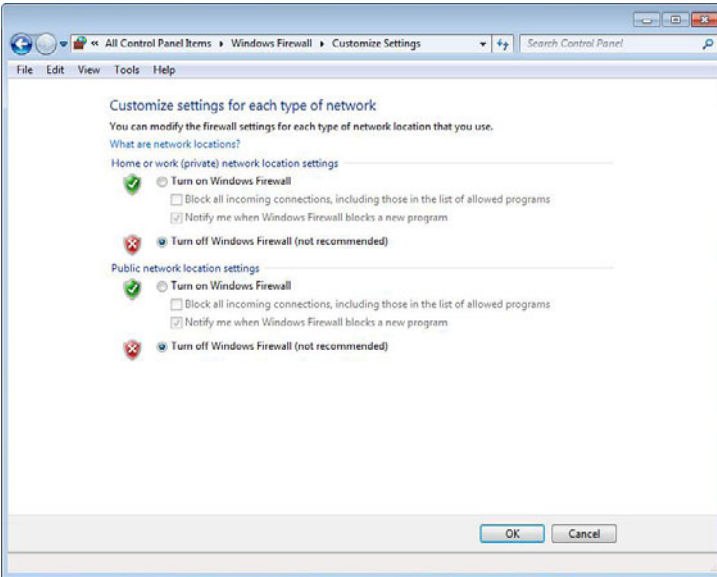


FIGURE 7.5 Setting Network Location in Windows Firewall.

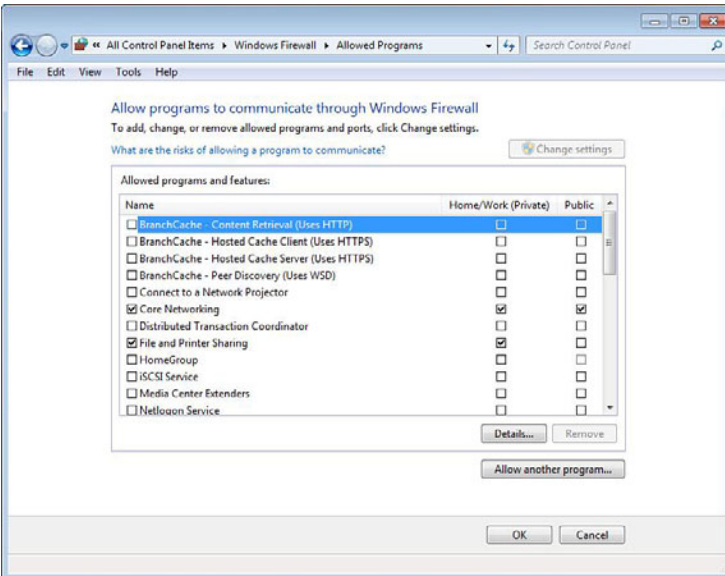


FIGURE 7.6 Allow programs to communicate through Windows Firewall.

**ExamAlert**

Remember if you want to use file and printer sharing, you need to allow File and Printer Sharing by using the Allow program to communicate through Windows Firewall option.

In addition to the notification setting available (configured by clicking Change notification settings) when you turn Windows Firewall on or off, you can display firewall notifications in the taskbar for three different behaviors:

- ▶ **Show icon and notifications:** The icon always remains visible on the taskbar in the notification area and notifications are displayed.
- ▶ **Hide icon and notifications:** The icon is hidden and notifications aren't displayed.
- ▶ **Only Show notifications:** The icon is hidden, but if a program needs to show a notification, it shows a notification balloon on the taskbar.

Notifications are also displayed in the Action Center in Control Panel.

## Windows Firewall with Advanced Security

The new Windows Firewall with Advanced Security is a Microsoft Management Console (MMC) snap-in that provides more advanced options for IT professionals. With this firewall, you can set up and view detailed inbound and outbound rules and integrate with Internet Protocol Security (IPsec). To access the Windows Firewall with Advanced Security, follow these steps:

1. Open Administrative Tools by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **Administrative Tools**.
2. Double-click **Windows Firewall with Advanced Security**, as shown in Figure 7.7. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

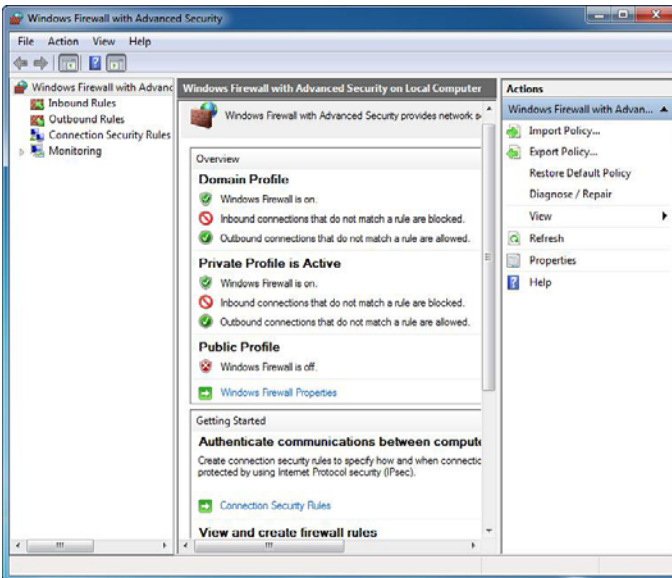


FIGURE 7.7 Windows Firewall with Advanced Security console.

You can also access the Windows Firewall with Advanced Security by clicking the **Advanced settings** option in the Windows Firewall screen. Of course, you must be a member of the Administrators group to use Windows Firewall with Advanced Security.

The Windows Firewall with Advanced Security management console enables you to configure the following:

- ▶ **Inbound rules:** Windows Firewall blocks all incoming traffic unless solicited or allowed by a rule, as shown in Figure 7.8.
- ▶ **Outbound rules:** Windows Firewall allows all outbound traffic unless blocked by a rule.
- ▶ **Connection security rules:** Windows Firewall uses a connection security rule to force two peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Connection security rules use IPsec to enforce security requirements.
- ▶ **Monitoring:** Windows Firewall uses the monitoring interface to display information about current firewall rules, connection security rules, and security associations.

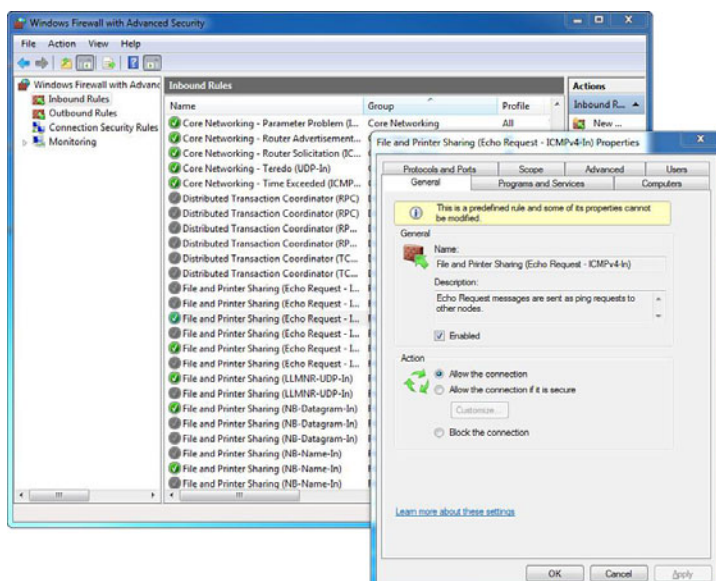


FIGURE 7.8 Inbound rules.

You create inbound rules to control access to your computer from the network. Inbound rules can prevent

- ▶ Unwanted software being copied to your computer.
- ▶ Unknown or unsolicited access to data on your computer.
- ▶ Unwanted configuration of your computer from remote locations.

To configure advanced properties for a rule using the Windows Firewall with Advanced Security, do the following:

1. Right-click the name of the inbound rule and then click **Properties**.
2. From the properties dialog box for an inbound rule, configure settings on the following tabs:
  - ▶ **General:** The rule's name, the program to which the rule applies, and the rule's action (allow all connections, allow only secure connections, or block).
  - ▶ **Programs and Services:** The programs or services to which the rule applies.
  - ▶ **Computers:** The computers that can communicate through the firewall.



- ▶ **Users:** The users that can communicate through the firewall.
- ▶ **Protocols and Ports:** The rule's IP protocol, source and destination TCP or UDP ports, and ICMP or ICMPv6 settings.
- ▶ **Scope:** The rule's source and destination addresses.
- ▶ **Advanced:** The profiles or types of interfaces to which the rule applies.

You can also use the Windows Firewall with Advanced Security to create outbound rules to control access to network resources from your computer.

Outbound rules can prevent

- ▶ Utilities on your computer from accessing network resources without your knowledge.
- ▶ Utilities on your computer from downloading software without your knowledge.
- ▶ Users of your computer from downloading software without your knowledge.

## Computer Connection Security Rules

Because the Internet is inherently insecure, businesses need to preserve the privacy of data as it travels over the network. Internet Protocol Security (IPsec) creates a standard platform to develop secure networks and electronic tunnels between two machines. The two machines are known as endpoints. After the tunnel has been defined and both endpoints agree on the same parameters, the data is encrypted on one end, encapsulated in a packet, and sent to the other endpoint where the data is decrypted.

In Windows XP and Windows Server 2003, you configure the Windows Firewall and IPsec separately. Unfortunately, because both can block or allow incoming traffic, it is possible that the Firewall and IPsec rules can conflict with each other. In Windows 7, Windows Firewall with Advanced Security provides a single, simplified interface for managing both firewall filters and IPsec rules.

Windows Firewall with Advanced Security uses authentication rules to define IPsec policies. No authentication rules are defined by default. To create a new authentication rule, follow these steps:

1. In Windows Firewall with Advanced Security, select the **Computer Connection Security Rules** node.
2. Right-click the **Computer Connection Security Rules** node in the console tree and then click **New Rule** to start the New Connection Security Rule Wizard.
3. From the Rule Type page of the New Authentication Rule Wizard (as shown in Figure 7.9), you can select the following:
  - ▶ **Isolation:** Used to specify that computers are isolated from other computers based on membership in a common Active Directory domain or current health status. You must specify when you want authentication to occur (for example, for incoming or outgoing traffic and whether you want to require or only request protection), the authentication method for protected traffic, and a name for the rule.
  - ▶ **Authentication exemption:** Used to specify computers that do not have to authenticate or protect traffic by their IP addresses.
  - ▶ **Server to server:** Used to specify traffic protection between specific computers, typically servers. You must specify the set of endpoints that exchange protected traffic by IP address, when you want authentication to occur, the authentication method for protected traffic, and a name for the rule.
  - ▶ **Tunnel:** Used to specify traffic protection that is tunneled, typically used when sending packets across the Internet between two security gateway computers. You must specify the tunnel endpoints by IP address, the authentication method, and a name for the rule.
  - ▶ **Custom:** Used to create a rule that does not specify a protection behavior. You would select this option when you want to manually configure a rule, perhaps based on advanced properties that cannot be configured through the pages of the New Authentication Rule Wizard. You must specify a name for the rule.

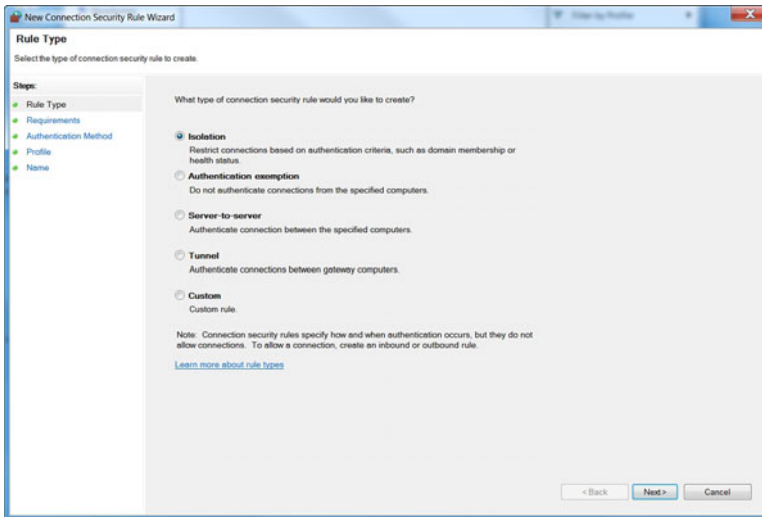


FIGURE 7.9 Specifying a new connection security rule.

To configure advanced properties for the rule, do the following:

1. Right-click the name of the rule and then click **Properties**.
2. From the properties dialog box for a rule, you can configure settings on the following tabs:
  - ▶ **General:** The rule's name and description and whether the rule is enabled.
  - ▶ **Computers:** The set of computers, by IP address, for which traffic is protected.
  - ▶ **Authentication:** When you want authentication for traffic protection to occur (for example, for incoming or outgoing traffic and whether you want to require or only request protection) and the authentication method for protected traffic.
  - ▶ **Advanced:** The profiles and types of interfaces to which the rule applies and IPsec tunneling behavior.

---

## Cram Quiz

1. Which Windows Firewall profile includes access to homegroups?
  - A. Home network
  - B. Work network
  - C. Public network
  - D. Internet network
  
2. If you need to configure IPsec, what program would you use in Windows 7?
  - A. IPsec Management console
  - B. Computer Management console
  - C. Windows Firewall with IPsec
  - D. Windows Firewall with Advanced Security

## Cram Quiz Answers

1. **A** is correct. The Home network location or profile is for home networks or when you know and trust the people and devices on the network. Network discovery is turned on for home networks, which enables you to see other computers and devices on the network. Answers B and C are incorrect because they have access to homegroups disabled. Answer D is incorrect because the Internet network is not a valid network location or profile.
  2. **D** is correct. The Windows Firewall with Advanced Security enables you to fine-tune the Windows Firewall and configure IPsec. Answer B is incorrect because you cannot configure IPsec with the Computer Management console. Answers A and C are incorrect because these consoles do not exist.
-

# Review Questions

- Which of the following does spyware not do?
  - A. Monitors keystrokes in an attempt to retrieve passwords and other private information
  - B. Changes the default home page to another site
  - C. Causes pop-up windows to appear frequently
  - D. Changes the polarity of your monitor, causing physical damage
  - E. Slows down your machine
- You work as a desktop technician at Acme.com. You have configured Windows Defender on all Microsoft Windows 7 machines on your domain. One user has an accounting application (which comes from a reputable company) that interacts with Microsoft Excel. When the application runs, an alert window opens up with a medium-level warning stating that the software might be spyware. You are sure that the application is not spyware. What do you need to do to stop these warnings from appearing? (Select the best answer.)
  - A. Open Windows Defender. Click Tools, click Options, and configure Windows Defender to ignore Medium alert items.
  - B. Configure Parental Controls to allow this application to run.
  - C. Open Windows Defender. Click Tools and click Options. Then under the Advanced options, click Add in the Do not scan these files or locations option. Then browse to the application executable. Click OK.
  - D. When the warning appears again, click Always Allow.
- When running Windows Defender, you are constantly alerted about specific software. What can you do so that you stop getting alerts for that software?
  - A. Run Windows full scan
  - B. Run Windows quick scan
  - C. Add the application to the allowed list
  - D. Add the item to the quarantine list
- You work as part of the IT support staff at Acme.com. You have a payroll application (PAY.EXE) that requires you to send data to the check printing company using TCP port 8787. What do you need to do to make this application able to function?
  - A. Open Windows Firewall and ensure that it is enabled. Add PAY.EXE to the exceptions list on the exceptions tab.
  - B. Open Windows Firewall and ensure that it is enabled. Add port 8787 to the exceptions list on the exceptions tab.

- C.** Open Windows Defender. Add PAY.EXE to the exceptions tab.
  - D.** Open Windows Defender. In Software Explorer, click the disable button for PAY.EXE.
5. Your corporation has several FTP servers. You need to make sure that a Windows 7 computer can only connect to the FTP servers when connected to the private network. What should you do?
- A.** Change the application control policies from the local policy
  - B.** Change the Advanced Sharing setting from the Network and Sharing Center Policy
  - C.** Change the Allowed Programs and Features list from the Windows Firewall Policy
  - D.** Create a new rule from the Windows Firewall with Advanced Security Policy
6. You create a shared folder called Docs on your computer running Windows 7. However, remote users cannot access the shared folder. What do you need to do to allow users to access the shared folder while keeping the system as secure as possible?
- A.** Disable Windows Defender
  - B.** Enable the File and Printer Sharing exception in the firewall setting
  - C.** Turn off the Windows Firewall
  - D.** Enable all incoming connections in the Windows Firewall
7. What should you do to prevent all inbound traffic to your computer running Windows 7 without the end user being notified?
- A.** Set the network location to Public
  - B.** Set the network location to Private
  - C.** Set the network location to domain
  - D.** Enable the Windows Firewall and select the Block all incoming connections checkbox
8. What do you call a firewall that monitors the state of active connections and uses the information gained to determine which network packets are allowed through the firewall?
- A.** Packet filter
  - B.** Stateful
  - C.** Stateless
  - D.** Packet analyzer

9. Which of the following statements is true?

- A. Windows Firewall is off by default.
- B. Windows Firewall is on by default.
- C. Windows Firewall is on by default if you install Windows Defender.
- D. Windows Firewall is only on if auditing is turned on.

10. What protocol enables you to create a standard platform to develop secure networks and electronic tunnels between two machines?

- A. Windows Firewall with Advanced Security
- B. Windows Defender
- C. Windows auditing
- D. Windows Tunnel Maker

# Review Question Answers

1. Answer **D** is correct. Spyware cannot physically damage a computer. It can, however, capture information as you type, change the default home page, generate pop-up windows, and slow your machine. Therefore, Answers A, B, C, and E are incorrect.
2. Answer **D** is correct. When you know that a program is not spyware, click Always allow so that Windows stops assuming the software is spyware. Answer A is incorrect because you don't want to ignore other programs that might be harmful. Answer B is incorrect because Parental Controls do not function on domains. Answer C is incorrect because Answer D is much easier to implement.
3. Answer **C** is correct. To stop an alert from being generated by a specific application, you need to add it to the allowed list. Answers A and B are incorrect because these choices do not cause an alert to stop for an application. Answer D is incorrect because if it is quarantined, the application is not able to run until it is removed from the quarantine folder and placed back to its original place.
4. Answer **A** is correct. Because you want the PAY.EXE to communicate through the firewall, you can use an exception where you can specify that PAY.EXE can communicate out port 8787. Answer B is incorrect because you want to specify that only PAY.EXE can communicate through port 8787, not any other programs. Answer C is incorrect because you want to add an exception to Windows Firewall, not to Windows Defender, which is used to protect against spyware. Answer D is incorrect because the Software Explorer was a component that was included with Windows Defender included with Windows Vista. Since then, Software Explorer has been discontinued with the version of Windows Defender that is included with Windows 7.
5. Answer **D** is correct. For more control on what the firewall allows and blocks, you use the Windows Firewall with Advanced Security Policy. Answers A and B are incorrect because you need to configure your firewall. Answer C is incorrect because FTP is not included in the list for programs included under the Windows Firewall with Advanced Security Policy.
6. Answer **B** is correct. When you use shared folders, you need to open the firewall to allow communication to the shared folders. Answer A is incorrect because Windows Defender protects against spyware. Answer C is incorrect because you do not want to turn off the firewall because it is not able to protect your system. Answer D is incorrect because allowing all incoming connections opens your computer to security breaches.
7. Answer **D** is correct. Enabling the Windows Firewall and selecting the Block all incoming connections checkbox prevents all inbound traffic for the specific network location. If you don't select the Notify me when Windows Firewall blocks a new program, you do not any notifications. Answers A, B, and C are incorrect because you need to select Block all incoming connections no matter which network location you choose.



8. Answer **B** is correct. A stateful firewall monitors the state of active connections and uses the information gained to determine which network packets are allowed through the firewall. Answer A is incorrect because a packet filter protects the computer by using an access control list (ACL), which specifies which packets are allowed through the firewall based on IP address and protocol (specifically the port number). Answer C is incorrect because a packet filter is a stateless firewall. Answer D is incorrect because a packet analyzer or protocol analyzer is used to capture and analyze individual packets.
9. Answer **B** is correct. Windows Firewall is turned on by default. Therefore, when trying to use applications that communicate on the network, they could be blocked. Because Windows Firewall is on by default, Answer A is incorrect. Answers C and D are incorrect because Windows Defender and auditing do not affect whether Windows Firewall is on or off.
10. Answer **A** is incorrect. IPsec, short for IP Security, is used to encrypt traffic between two end points. To configure both the firewall and IPsec, you use the Windows Firewall with Advanced Security. Answer B is incorrect because the Windows Defender protects against spyware. Answer C is incorrect because Windows auditing is used to check what activities are happening to the system or object. Answer D is incorrect because there is no Windows Tunnel Maker program.

## CHAPTER 8

# User Management

**This chapter covers the following 70-680 Objectives:**

- ▶ Configure user account control (UAC)
- ▶ Configure authentication and authorization
- ▶ Configure remote connections

To keep a system secure, you need to use user accounts, which provide accountability and the ability to give rights and permissions to individuals. If your computer has many users, you can then use groups to simplify the granting of rights and permissions by assigning users to groups and then assigning the rights and permissions to those groups. To make your system secure, Windows 7 includes *User Account Control* to help protect against malware that might attack your system at any time by expanding what a standard user can do on a system without becoming an administrator.

# Authentication and Authorization

## ► Configure authentication and authorization

### CramSaver

1. What is the process used to confirm a user's identity?
  - A. Authentication
  - B. Authorization
  - C. Auditing
  - D. Certificate
2. Which local user accounts are automatically created when you install a fresh copy of Windows 7 and are also disabled by default? (Choose all that apply.)
  - A. Administrator
  - B. Administrators
  - C. Remoteldentity
  - D. Guest

### Answers

1. **A** is correct. Authentication is the process used to confirm a user's identity, when he or she accesses a computer system or additional system resources. Answer B is incorrect because authorization occurs after authentication, which allows access to a network resource. Answer C is incorrect because auditing is the recording of activity to be used to track user actions. Answer D is incorrect because a digital certificate is a form of authentication.
2. **A** and **D** are correct. The built-in administrator account provides complete access to files, directories, and services. The Guest account is designed for users who need one-time or occasional access. The Administrator and Guest accounts are disabled by default. Answer B is incorrect because Administrators is a group, not an account. Answer C is incorrect because there is no user account called Remoteldentity.

Authentication is the process used to confirm a user's identity when he or she accesses a computer system or an additional system resource. The most common authentication method is using a username and password. When working

with transactions over the Internet that deal with money, credit cards, or personal information, username/password authentication has an inherent weakness given its susceptibility to passwords that can be stolen, accidentally revealed, or hacked.

Because of this weakness, these transactions usually employ digital certificates to prove the identity of users or companies and also contain an encryption key, which is used to encrypt data sent over the Internet.

Users must be authenticated to verify their identity when accessing files or other network resources over the network. The Windows 7 operating system includes the following authentication methods for network logons:

- ▶ **Kerberos version 5 protocol:** The main logon authentication method used by clients and servers running Microsoft Windows operating systems. It is used to authenticate both user accounts and computer accounts.
- ▶ **Windows NT LAN Manager (NTLM):** Used for backward compatibility with pre-Windows 2000 operating systems and some applications. It is less flexible, efficient, and secure than the Kerberos version 5 protocol.
- ▶ **Certificate mapping:** Typically used in conjunction with smart cards for logon authentication. The certificate stored on a smart card (about the size of a credit card) is linked to a user account for authentication. A smart card reader is used to read the smart card and authenticate the user.

After you have authentication proving who or what an identity is, you can then use authorization, which allows a system to determine whether an authenticated user can access a resource and how they can access the resource.

A right authorizes a user to perform certain actions on a computer, such as logging on to a system interactively/locally to the computer, backing up files and directories, performing a system shutdown, or adding/removing a device driver. Administrators can assign specific rights to individual user accounts or group accounts. Rights are managed with the User Rights policy. For Windows Server 2008, you can find user rights by opening the group policy via the Group Policy Management console, opening Computer Configuration, opening Windows Settings, opening Security Settings, opening Local Policies, and opening User Rights Assignment.

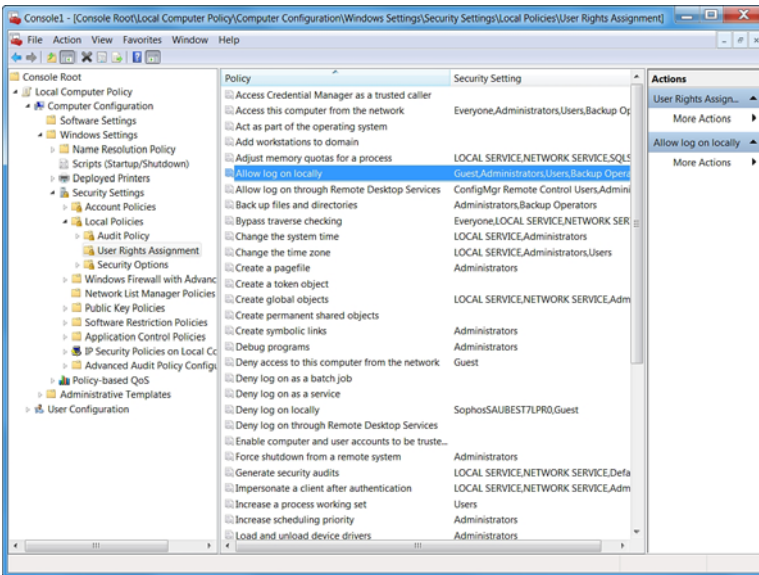


FIGURE 8.1 User rights.

A permission defines the type of access granted to an object or object attribute. The permissions available for an object depend on the type of object. For example, a user has different permissions than a printer, which has different permissions than a file or folder on an NTFS volume. When a user or service tries to access an object, its access is granted or denied by an Object Manager. File and Folder permissions as well as Shared permissions are handled by Windows Explorer.

## User Accounts and Groups

Microsoft Windows 7 workstations can be configured as a member of a workgroup or member of a domain. When a workstation is configured as a member of a workgroup, user access and security are configured on the workstation itself. Each computer maintains its own security database, which includes its own local user accounts and groups. If a user on one computer needs to access resources on other computers, a user account has to be created on each computer. The user and group information is not shared with other computers.

A *domain* is a logical unit of computers and network that define a security boundary. A domain uses one database known as Active Directory, which is stored on one or more domain controllers. It gives the capability to share its common security and user and group account information for all computers

within the domain. When a user logs onto the domain, he or she can access resources throughout the domain with the same logon (single sign-on). The domain allows for centralized network administration of all users, groups, and resources on the network.

A user account enables a user to log on to a computer or domain with an identity that can be authenticated and authorized for access to the resources of the computer or domain. Because the user account is meant to be assigned to one and only one user, it enables you to assign rights and permissions to a single user and gives you the ability to track what users are doing (accountability).

#### Note

It is highly recommended that all users who log on to the network should have their own unique user account and password.

Two general types of user accounts are defined in Windows 7:

- ▶ **Local user accounts:** User accounts defined on a local computer, which have access to the local computer only. You add or remove local user accounts with Control Panel's User Accounts options or the Local Users and Groups utility. Local Users and Groups is accessible through the Computer Management console, a Microsoft Management Console (MMC) tool that is found in Administrative tools.
- ▶ **Domain user accounts:** User accounts are defined in the Active Directory. Through single sign-on, these accounts can access resources throughout a domain/forest. When a computer is a member of an Active Directory domain, you can create domain user accounts using Active Directory Users and Computers. This MMC tool is available on the Administrative Tools menu when you install the Microsoft Remote Server Administration Tools (RSAT) for Windows 7 on your Windows 7 computer. RSAT can be found at <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d>.

A local user account allows users to log on at and gain access to resources on only the computer where they create the account. The user account tells Windows what files and folders the user can access, what changes you can make to the computer, and your personal preferences, such as your desktop background or color theme. User accounts enable you to share a computer with several people, but still have your own files and settings. Each person accesses his or her user account with a user name and password.

## Default User Accounts

Every Windows 7 computer has local computer accounts, regardless of whether the computer is a member of a workgroup or a domain. When you install Windows 7, the operating system installs default user accounts, which are managed using the User Accounts applet. The key accounts you see are as follows:

- ▶ **Administrator:** Administrator is a predefined account that provides complete access to files, directories, services, and other facilities on the computer. You can't delete this account.
- ▶ **Guest:** Guest is designed for users who need one-time or occasional access. Although guests have only limited system privileges, you should be very careful about using this account because it opens the system to potential security problems. The risk is so great that the account is initially disabled when you install Windows 7.

The built-in administrator account is disabled by default in Windows 7 on new installations. If Windows 7 determines during an upgrade from Windows Vista that the built-in administrator is the only active local administrator account, Windows 7 leaves the account enabled and places the account in Admin Approval Mode. The built-in administrator account, by default, cannot log on to the computer in safe mode.

Windows 7 also provides groups, which you use to grant permissions to similar types of users and to simplify account administration. If a user is a member of a group that can access a resource, that particular user can access the same resource. Thus, you can give a user access to various work-related resources just by making the user a member of the correct group.

## Windows 7 Local Accounts

When you create additional accounts in Windows 7 using the Control Panel, you choose between two different kinds of accounts:

- ▶ Standard user
- ▶ Administrator

Each account type gives the user a different level of control over the computer.

The standard user account is the account to use for everyday computing. A standard user account lets a person use most of the capabilities of the computer, but permission from an administrator is required if you want to make

changes that affect other users or the security of the computer. You can use most programs that are installed on the computer, but you can't install or uninstall software and hardware, delete files that are required for the computer to work, or change settings on the computer that affect other users. If you're using a standard user account, some programs might require you to provide an administrator password before you can perform certain tasks.

The administrator account provides the most control over the computer, and should be used only when necessary. The administrator account lets you make changes that affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. Administrators can also make changes to other local user accounts.

### Note

When you create an administrator user, it adds the user to the Administrator group. When you create a standard user, it adds the user to the Users group.

When you set up Windows, you are required to create a user account. This account is an administrator account that allows you to set up your computer and install any programs that you want to use. After you have finished setting up your computer, recommended practice dictates that you use a standard user account for your day-to-day computing.

### ExamAlert

Because the administrator account has access to all network resources on the computer, it is always more secure to use a standard user account instead of an administrator account to do normal day-to-day tasks.

The guest account is primarily for people who need temporary access to the computer. The guest account is for users who don't have a permanent account on your computer or domain. It allows people to use your computer without having access to your personal files. People using the guest account can't install software or hardware, change settings, or create a password.

### Note

By default, the guest account is disabled. Therefore, you have to enable the guest account before it can be used.



All user accounts are identified with a logon name. In Windows 7, this logon name has two parts: the user name and the user's computer name or domain in which the user account exists. If you have a computer called PC1 and the username is called User1, the full logon name for Windows 7 is PC1\User1. Of course, User1 could log on to his or her local workstation and access local resources but would not be able to access domain resources.

When working with domains, the full logon name can be expressed in two different ways:

- ▶ The user account name and the full domain name separated by the at sign (@). For example, the full logon name for User1 in the Acme.com domain would be User1@Acme.com.
- ▶ The user account name and the domain separated by the backslash symbol (\). For example, the full logon name for User1 in the Acme domain would be Acme\User1.

Although Windows 7 represents a user account with a user name, the accounts key identifier is the security identifier (SID). SIDs are unique identifiers that are automatically generated when a user account is created. They consist of a computer or domain security ID prefix combined with a unique relative ID for the user. Having a unique identifier enables you to change user names. It also enables you to delete accounts without worrying that someone might gain access to resources simply by re-creating an account.

To provide security, user accounts can have passwords. Passwords are authentication strings for an account that consist of upper- and lowercase characters, digits, and special characters.

### ExamAlert

It is recommended that all local computer accounts have passwords. If an account is created without a password, anyone can log on to the account, and there is no protection for the account. However, a local account without a password cannot be used to remotely access a computer.

**Note**

It is always recommended that you use a strong password or a complex password. Microsoft defines a complex password used in group policies as

- ▶ Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- ▶ Passwords must be at least six characters in length or the number of characters specified in the Minimum password length policy setting.
- ▶ Passwords must contain characters from at least three of the following four categories:
  - ▶ English uppercase alphabet characters (A–Z)
  - ▶ English lowercase alphabet characters (a–z)
  - ▶ Base 10 digits (0–9)
  - ▶ Non-alphanumeric characters (for example, !\$,%,%)

Group policies can be used to enforce using complex passwords.

## Managing Local Logon Accounts

The User Accounts console accessed through the Control Panel, as shown in Figure 8.2, provides an easy way to manage the user accounts. If you want more advanced control, you use the Users and Groups console (which is also part of the Computer Management console).

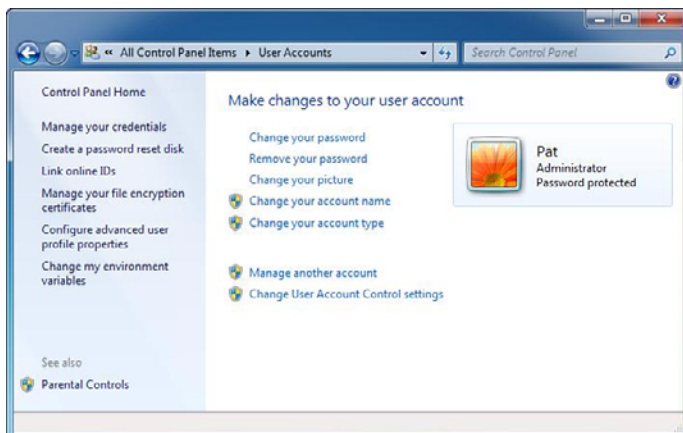


FIGURE 8.2 User Accounts console.

For a computer that is a member of a workgroup, you can create a local user account on a computer by following these steps:

1. In the Control Panel, click **Add or Remove User Accounts** under the User Accounts heading. This displays the Manage Accounts page, as shown in Figure 8.3. The Manage Accounts page lists all configurable user accounts on the local computer by account type with configuration details. If an account has a password, it is listed as being password protected. If an account is disabled, it is listed as being off.
2. Click **Create a new account**. This displays the Create New Account page.
3. Type the name of the local account. This name is displayed on the Welcome screen and Start menu.
4. Set the type of account as either Standard User or Administrator from the screen shown in Figure 8.4. To give the user full permissions on the local computer, select **Administrator**.

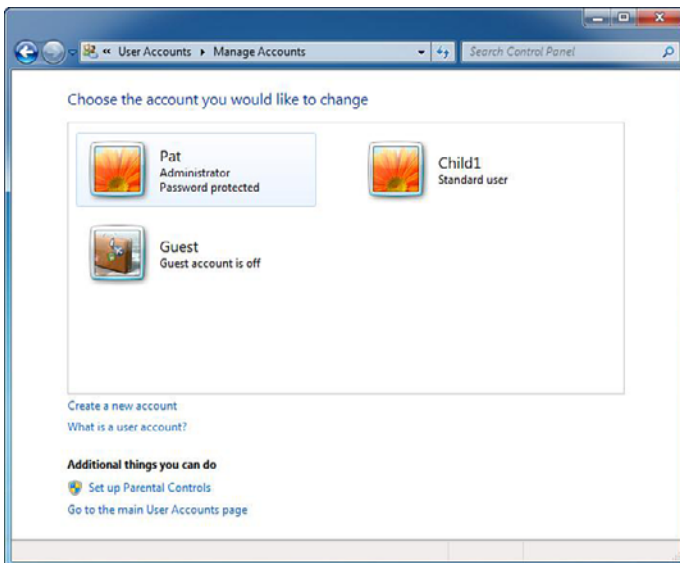


FIGURE 8.3 Manage accounts.

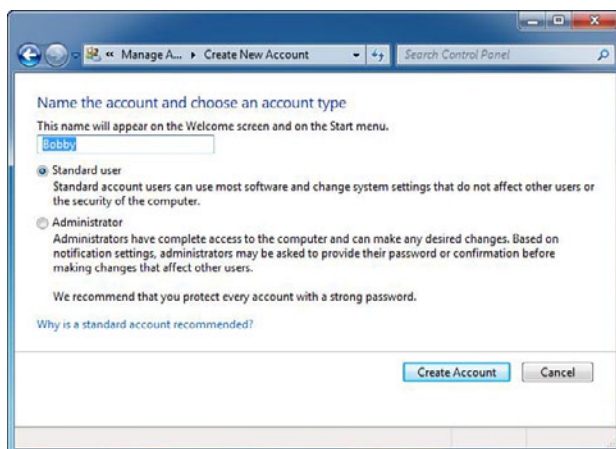


FIGURE 8.4 Selecting the account type.

If a user needs to be able to log on locally to a computer and has an existing domain account, you can grant the user permission to log on locally by completing the following steps:

1. In Control Panel, click User Accounts. On the User Accounts page, click the **Give other users access to this computer** link. This displays the User Accounts dialog box, as shown in Figure 8.5. The User Accounts dialog box lists all configurable user accounts on the local computer by account type with group membership details.

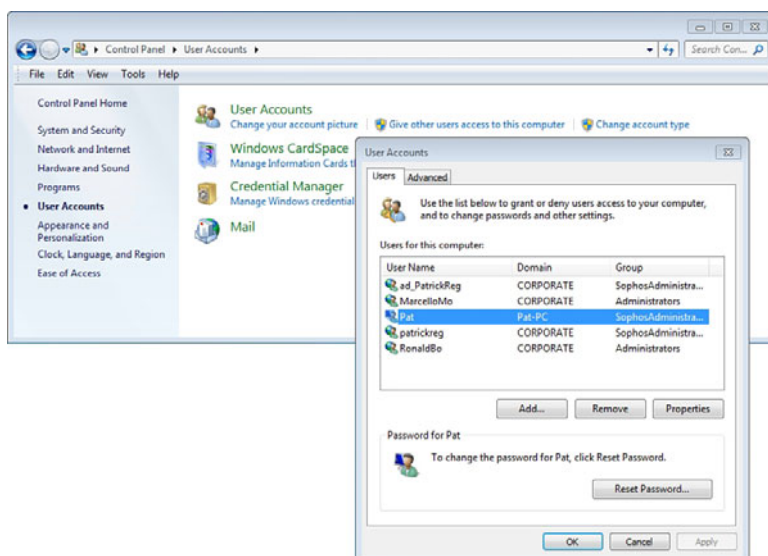


FIGURE 8.5 User Accounts dialog box.

2. Click **Add**. This starts the Add New User Wizard.
3. You are creating a local computer account for a user with an existing domain account. Type the user's domain account name and domain in the fields provided.
4. Using the options provided, select the type of user account, administrator, standard user or Other account. An Other account is created as a member of the specific group you choose. To give the user the permissions of a specific group, select **Other** and then select the desired group.
5. Click **Finish**.

You can change the account type for a local computer user by completing the following steps:

1. In Control Panel, click **Add or Remove User Accounts** under the User Accounts heading. This displays the Manage Accounts page.
2. Click the account you want to change and then click **Change the Account Type**.
3. On the Change the Account Type page, set the level of access for the user as either Standard User or Administrator and then click **Change the Account Type**.

In a domain, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, click **User Accounts**. On the User Accounts page, click the **Change account type** link. This displays the User Accounts dialog box.
2. On the Users tab, click the user account you want to work with and then click **Properties**.
3. In the Properties dialog box, select the **Group Membership** tab.
4. Select the type of account as **Standard User** or **Administrator**. Or select **Other** and then select the desired other group.
5. Click **OK** twice.

When the computer is not part of a domain (workgroup configuration), by default, local users are created without passwords. Therefore, if you click the account name on the Welcome screen on an account that does not have a password, you are automatically logged in.

You can create a password for a local user account by completing the following steps:

1. Log on as the user whose password you want to create. In Control Panel, click **Add or Remove User Accounts** under the User Accounts heading. This displays the Manage Accounts page.
2. All user accounts available on the machine are shown, and you need to click the account you want to work with. To prevent possible data loss, this should be the same as the account under which you are currently logged on. Any account that has a current password is listed as Password Protected. Any account without this label doesn't have a password.
3. Click **Create a Password**. Type a password and then confirm it. Afterward, type a unique password hint. The password hint is a word or phrase that can be used to obtain the password if it is lost. This hint is visible to anyone who uses the computer.
4. Click **Create Password**.

In a workgroup, you can remove a user's local account and effectively deny logon by completing these steps:

1. Log on as a user with local administrator privileges. In Control Panel, click **Add or Remove User Accounts** under the User Accounts heading. This displays the Manage Accounts page.
2. Click the account you want to remove.
3. Click **Delete the Account**.
4. Before deleting the account, you have the opportunity save the contents of the user's desktop and Documents folder to a folder on the current user's desktop. To save the user's documents, click **Keep Files**. To delete the files, click **Delete Files**.
5. Confirm the account deletion by clicking **Delete Account**. Keep in mind that in a domain, unless there are further restrictions with regard to logon workstations, a user might still be able to gain access to the workstation by logging on with a domain account.

To access the Users and Groups in the Computer Management console, do the following:

1. Click the **Start** button.
2. Click **Control Panel**.

3. Click **System and Maintenance**.
4. Click **Administrative Tools**.
5. Click **Computer Management**.
6. Double-click **Local Users and Groups**.
7. Select either **Users** (shown in Figure 8.6) or **Groups** (shown in Figure 8.7).

To create a user or group, just right-click **Users** or **Groups** and select **New User** or **New Group**. To modify a user or group, double-click on the identity.

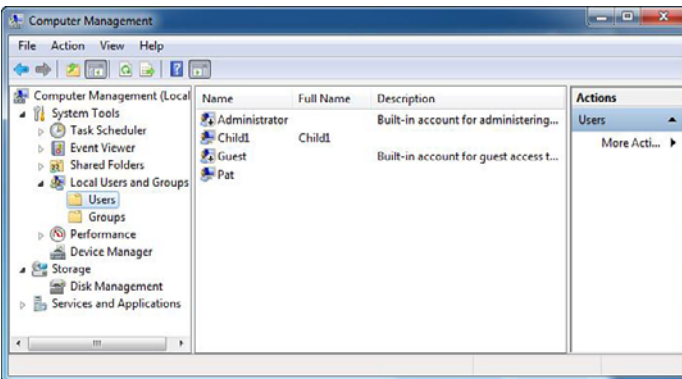


FIGURE 8.6 Managing Users with Computer Management console.

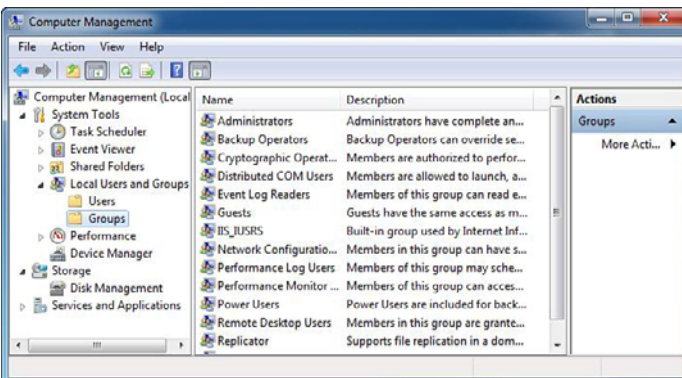


FIGURE 8.7 Managing Groups with Computer Management console.

# Credential Manager

Credential Manager enables you to store credentials, such as user names and passwords, so that the next time you or an application that you are using accesses a website or network resource, the credentials are automatically applied so that you can access the website or network resource automatically. Credentials are saved in special folders on your computer called vaults.

To add a password to your Windows vault:

1. Open **User Accounts** in the Control Panel.
2. In the left pane, click **Manage your credentials**. You see the screen shown in Figure 8.8.

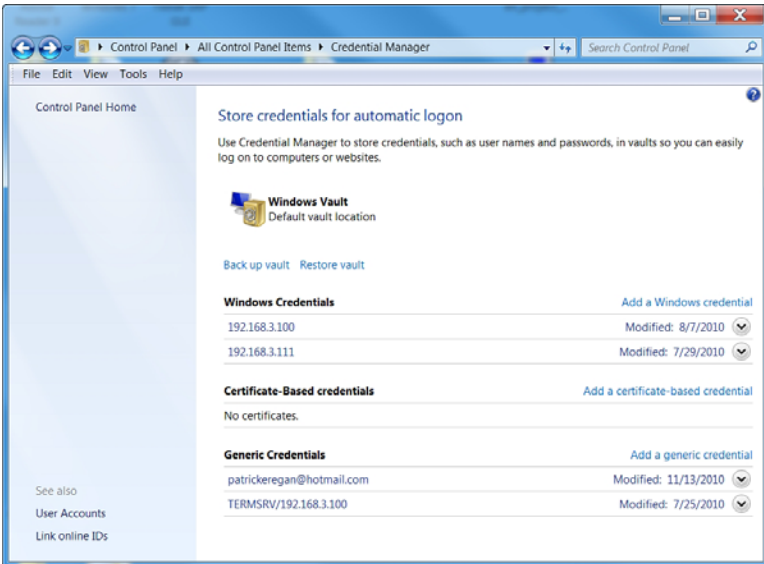


FIGURE 8.8 Credential Manager.

3. Click **Add a Windows credential**.
4. In the Internet or network address box, type the name of the computer on the network that you want to access, as shown in Figure 8.9.



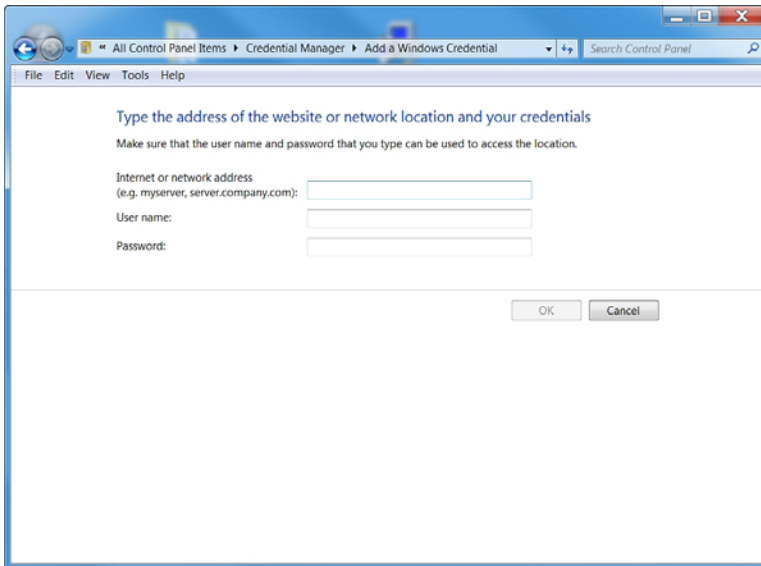


FIGURE 8.9 Adding a Windows credential.

5. In the User name and Password boxes, type the user name and password that you use for the computer or websites and then click **OK**.

---

## Cram Quiz

1. What authorizes a user to perform certain actions on a computer such as logging on to a system interactively, backing up files, or performing a system shutdown?
  - A. A right
  - B. A permission
  - C. A digital certificate
  - D. Auditing ability
2. Where do you locate the User Accounts console?
  - A. Accessories
  - B. Maintenance
  - C. Control Panel
  - D. System Properties

## Cram Quiz Answers

1. **A** is correct. A right authorizes a user to perform certain actions on the computer. Answer B is incorrect because a permission defines the type of access granted to an object or object attribute. Answer C is incorrect because a digital certificate is used for authentication. Answer D is incorrect because auditing is used to track user actions and activities.
  2. **C** is correct. To create and manage users in Windows 7, you usually use the User Accounts console from the Control Panel. You will not find any tools to manage users in Accessories, Maintenance, or System Properties. Therefore, the other answers are incorrect.
-

# User Account Control

## ► Configure authentication and authorization

### CramSaver

1. What feature prevents a program from making unauthorized changes to your computer running Windows 7?
  - A. UAC
  - B. USB
  - C. GMT
  - D. ActiveX
2. Which UAC slider option dims the desktop causing other programs not to run when the UAC dialog box appears? (Choose all that apply.)
  - A. Always notify
  - B. Notify me only when programs try to make changes to my computer
  - C. Notify me only when programs try to make changes to my computer (do not dim my desktop)
  - D. Never notify

### Answers

1. **A** is correct. User Account Control (UAC) is a feature in Windows that can help prevent unauthorized changes to your computer. If you are logged in as an administrator, UAC asks you for permission, and if you are logged in as a standard user, UAC asks you for an administrator password before performing actions that could potentially affect your computer's operation or that change settings that affect other users. Answer B is incorrect because USB is short for Universal Serial Bus, which is used to connect devices to the computer. Answer C is incorrect because Greenwich Mean Time (GMT) is used with time zones. Answer D is incorrect because ActiveX is a framework for defining reusable components known as controls.
2. **A** is correct. The only option that dims the screen when a UAC prompt appears is Always notify; therefore, all other answers are incorrect.

Need-to-know is a basic security concept that says information should be limited to only those individuals who require it, and they should be given only enough access to carry out their specific job functions. When planning for how you assign the rights and permissions to the network resources, follow these two main rules:

- ▶ Give the rights and permissions for the user to do his or her job.
- ▶ Don't give any additional rights and permissions that a user does not need.

Although you want to keep resources secure, you want to make sure that the users can easily get what they need. For example, give users access to the necessary files, and give them only the permissions they need. If they need to read a document but don't need to make changes to it, they need to have only the read permission. Giving a person or group only the required amount of access and nothing more is known as the rule or principle of least privilege.

When you ran earlier versions of Windows, including Windows XP, and you logged in with an administrative account, every task that you execute and every process that ran in the account's session ran as an administrator with elevated privileges. Because the elevated privileges provided access to everything, it opened the possibility of human error, which could cause problems in Windows functionality or data loss, and it allowed malicious software to access any part of the computer. Unfortunately, most legacy applications and even new applications were or are not designed to work without full administrator privileges.

User Account Control (UAC) is a feature in Windows that can help prevent unauthorized changes to your computer. If you are logged in as an administrator, UAC asks you for permission, and if you are logged in as a standard user, UAC asks you for an administrator password before performing actions that could potentially affect your computer's operation or that change settings that affect other users. When you see a UAC message, read it carefully and then make sure the name of the action or program that's about to start is one that you intended to start.

The Application Information Service (AIS) is a system service that facilitates UAC and launching applications that require one or more elevated privileges or user rights to run, such as Administrative Tasks, as well as applications that require higher integrity levels. If you disable AIS, when you try to run applications that require administrative access, you get an Access Denied error.

To keep track of a user's access, when a standard user logs in to Windows 7, a token is created that contains only the most basic privileges assigned. When an administrator logs in, two separate tokens are assigned. The first token contains all privileges typically awarded to an administrator, and the second is a restricted token similar to what a standard user receives. User applications, including the Windows Shell, are then started with the restricted token resulting in a reduced privilege environment even under an Administrator account.

When an application requests elevation or is run as administrator, UAC prompts for confirmation and, if consent is given, starts the process using the unrestricted token.

The default UAC setting allows a standard user to perform the following tasks without receiving a UAC prompt:

- ▶ Install updates from Windows Update
- ▶ Install drivers from Windows Update or those that are included with the operating system
- ▶ View Windows settings
- ▶ Pair Bluetooth devices with the computer
- ▶ Reset the network adapter and perform other network diagnostic and repair tasks

Administrative users automatically have:

- ▶ Read/Write/Execute permissions to all resources
- ▶ All Windows privileges

When your permission or password is needed to complete a task, UAC alerts you with one of the following messages:

- ▶ **A setting or feature that is part of Windows needs your permission to start:** A Windows function or program that can affect other users of this computer needs your permission to start. Check the name of the action to ensure that it's a function or program you want to run.
- ▶ **A program that is not part of Windows needs to your permission to start:** A program that's not part of Windows needs your permission to start. It has a valid digital signature indicating its name and its publisher, which helps to ensure that the program is what it claims to be. Make sure that this is a program that you intended to run.
- ▶ **A program with an unknown publisher) needs your permission to start** (see Figure 8.10): An unidentified program is one that doesn't have a valid digital signature from its publisher to ensure that the program is what it claims to be. This doesn't necessarily indicate danger, as many older, legitimate programs lack signatures. However, you should use extra caution and only allow this program to run if you obtained it from a trusted source, such as the original CD/DVD or a publisher's website.

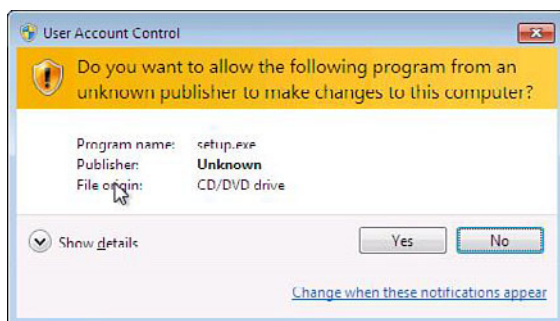


FIGURE 8.10 User Account Control alert.

- ▶ **You have been blocked by your system administrator from running this program:** This is a program that your administrator has specifically blocked from running on your computer. To run this program, you must contact your administrator and ask to have the program unblocked. Of course, it is recommended that you log on to your computer with a standard user account most of the time. With a standard user account, you can run standard business applications such as a word processor or spreadsheet, surf the Internet, or send email. When you want to perform an administrative task, such as installing a new program or changing a setting that affects other users, you don't have to switch to an administrator account. Windows prompts you for permission or an administrator password before performing the task.

To help protect your computer, you can create standard user accounts for all the users who share the computer. When someone who has a standard account tries to install software, Windows asks for an administrator account's password so that software can't be installed without the user's knowledge and permission.

UAC can be enabled or disabled for any individual user account. If you disable UAC for a user account, you lose the additional security protections UAC offers and put the computer at risk. To enable or disable UAC for a particular user account, follow these steps:

1. In Control Panel, click **User Accounts**.
2. On the User Accounts page, click **User Accounts**.
3. Click **Change User Account Control settings**.
4. Move the slider to the appropriate options, as shown in Figure 8.11 and Table 8.1.

- When prompted to restart the computer, click **Restart Now** or **Restart Later** as appropriate for the changes to take effect.

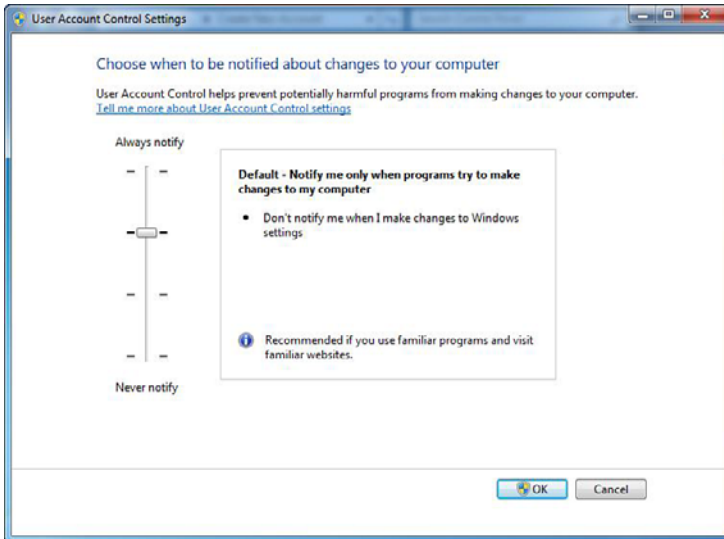


FIGURE 8.11 User Account Control settings.

TABLE 8.1 UAC Settings

Setting	Description	Security Impact
Always notify	<p>You are notified before programs make changes to your computer or to Windows settings that require the permissions of an administrator.</p> <p>When you're notified, your desktop is dimmed, and you must either approve or deny the request in the UAC dialog box before you can do anything else on your computer. The dimming of your desktop is referred to as the <i>secure desktop</i> because other programs can't run while it's dimmed.</p>	<p>This is the most secure setting.</p> <p>When you are notified, you should carefully read the contents of each dialog box before allowing changes to be made to your computer.</p>

TABLE 8.1 Continued

Setting	Description	Security Impact
Notify me only when programs try to make changes to my computer	<p>You are notified before programs make changes to your computer that require the permissions of an administrator.</p> <p>You are not notified if you try to make changes to Windows settings that require the permissions of an administrator.</p> <p>You are notified if a program outside of Windows tries to make changes to a Windows setting.</p>	<p>It's usually safe to allow changes to be made to Windows settings without you being notified. However, certain programs that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these programs to install files or change settings on your computer. You should always be careful about which programs you allow to run on your computer.</p>
Notify me only when programs try to make changes to my computer (do not dim my desktop)	<p>You are notified before programs make changes to your computer that require the permissions of an administrator.</p> <p>You are not notified if you try to make changes to Windows settings that require the permissions of an administrator.</p> <p>You are notified if a program outside of Windows tries to make changes to a Windows setting.</p>	<p>This setting is the same as to make changes to my computer, but you are not notified on the secure desktop.</p> <p>Because the UAC dialog box isn't on the secure desktop with this setting, other programs might be able to interfere with the dialog's visual appearance. This is a small security risk if you already have a malicious program running on your computer.</p>



TABLE 8.1 **Continued**

Setting	Description	Security Impact
Never notify	<p>You are not notified before any changes are made to your computer. If you are logged on as an administrator, programs can make changes to your computer without you knowing about it.</p> <p>If you are logged on as a standard user, any changes that require the permissions of an administrator are automatically denied.</p> <p>If you select this setting, you need to restart the computer to complete the process of turning off UAC. After UAC is off, people who log on as administrator always have the permissions of an administrator.</p>	<p>This is the least secure setting. When you set UAC to never notify, you open your computer to potential security risks.</p> <p>If you set UAC to Never notify, you should be careful about which programs you run, because they have the same access to the computer as you do. This includes reading and making changes to protected system areas, your personal data, saved files, and anything else stored on the computer. Programs are also able to communicate and transfer information to and from anything your computer connects with, including the Internet.</p>

**Note**

UAC can prevent you from saving files to the root directory of your hard drive.

Besides enabling or disabling UAC, you control the behavior of the UAC by using local or group policies. Local policies are managed from each local computer while group policies are managed as part of Active Directory. Table 8.2 defines the settings found in local and group policies.

TABLE 8.2 **UAC Policy Settings Available in the Policy Editor Snap In**

Policy	Security Settings
Admin Approval Mode for the Built-in Administrator account	<p>Enabled</p> <p><i>Disabled (Default)</i></p>
Behavior of the elevation prompt for administrators in Admin Approval Mode	<p>Elevate without prompting</p> <p>Prompt for credentials</p> <p><i>Prompt for consent (Default)</i></p>

TABLE 8.2 **Continued**

<b>Policy</b>	<b>Security Settings</b>
Behavior of the elevation prompt for standard users	Automatically deny elevation requests <i>Prompt for credentials (Default)</i>
Detect application installations and prompt for elevation	<i>Enabled (Default)</i> Disabled
Only elevate executables that are signed and validated	Enabled <i>Disabled (Default)</i>
Only elevate UIAccess applications that are installed in secure applications	<i>Enabled (Default)</i> Disabled
Run all administrators in Admin Approval Mode	<i>Enabled (Default)</i> Disabled
Switch to the secure desktop when prompting for elevation	<i>Enabled (Default)</i> Disabled
Virtualize file and registry write failures to per-user locations	<i>Enabled (Default)</i>

To change the behavior of the User Account Control message for administrators in Admin Approval Mode:

1. Click **Start**, type `secpol.msc` in the Search programs and files box, and press **Enter**.
2. If UAC is currently configured in Admin Approval Mode, the User Account Control message displays. Click **Continue**.
3. From the Local Security Policy tree, click **Local Policies** and then double-click **Security Options**.
4. Scroll down to and double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**.
5. From the drop-down menu, select one of the following settings:
  - ▶ **Elevate without prompting:** In this case, applications that have been marked as administrator applications, as well as applications detected as setup applications, automatically run with the full administrator access token. All other applications automatically run with the standard user token.

- ▶ **Prompt for credentials:** In this case, in order to give consent for an application to run with the full administrator access token, the user must enter administrator credentials. This setting supports compliance with Common Criteria or corporate policies.
- ▶ **Prompt for consent:** This is the default setting.

6. Click **Apply**.

Use the following procedure to change the User Account Control message behavior for standard users:

1. Click **Start**, type `secpol.msc` in the Search programs and files box, and press **Enter**.
2. If UAC is currently configured to prompt for administrator credentials, the User Account Control message displays. Click **Continue**.
3. From the Local Security Policy tree, click **Local Policies** and then double-click **Security Options**, as shown in Figure 8.12.
4. Scroll down and double-click **User Account Control: Behavior of the elevation prompt for standard users**.
5. From the drop-down menu, select one of the following settings:
  - ▶ **Automatically deny elevation requests:** In this case, administrator applications are not able to run. The user should see an error message from the application that indicates a policy has prevented the application from running.
  - ▶ **Prompt for credentials:** This is the default setting. In this case, for an application to run with the full administrator access token, the user must enter administrator credentials.
6. Click **Apply**.

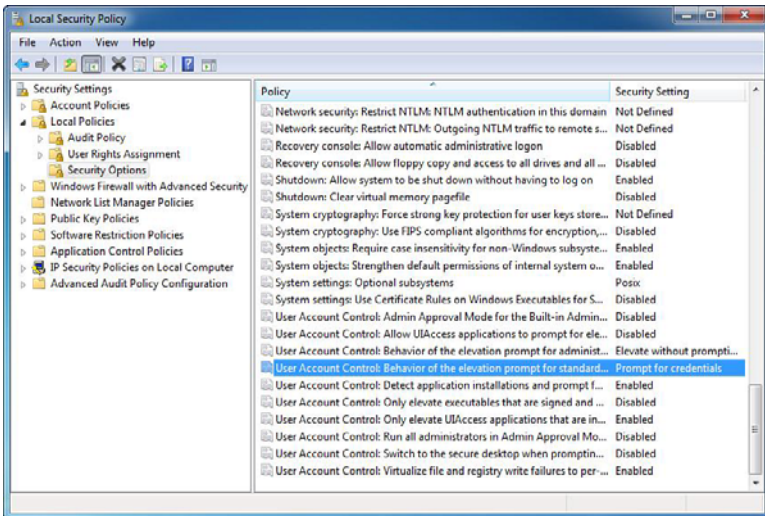


FIGURE 8.12 Controlling UAC with Group Policies.

## Cram Quiz

- You download a software package from the Internet and decide to install it. What would you use to ensure that the software package does not make changes that you are not aware of?
  - A. Windows Defender
  - B. Windows Firewall
  - C. User Account Control
  - D. System Configuration
- You are logged in as a local administrator. You are trying to save a file to C:\ but you are denied. What could be the cause?
  - A. Windows Defender
  - B. Windows Firewall
  - C. User Account Control
  - D. Software Explorer

## Cram Exam Answers

- 1. C** is correct. User Account Control prompts you if a program tries to make a system change, including installing additional software. Answer A is incorrect because Windows Defender is used to protect against spyware. Answer B is incorrect because Windows Firewall blocks traffic that should not go through the firewall. Answer D is incorrect because it is used to manage which programs start during boot.
  - 2. C** is correct. User Account Control is used to make sure software does not make any system changes without your knowledge or administrative permission. It can also prevent you from saving files to the C drive root directory. Answer A is incorrect because Windows Defender is used to protect against spyware. Answer B is incorrect because Windows Firewall blocks traffic that should not go through the firewall. Answer D is incorrect because Software Explorer was part of Windows Defender that came with Windows Vista but was discontinued with Windows 7.
-

# Security Auditing

► **Configure remote connections**

## CramSaver

1. What feature tracks and records various security-related events so that you can detect intruders and attempts to compromise the system?
  - A. Auditing
  - B. ACL
  - C. Permissions
  - D. Rights
2. You want to enable auditing of a folder called Reports. What is the first step you need to do?
  - A. Enable user auditing
  - B. Enable file auditing
  - C. Enable object auditing
  - D. Enable ACL auditing

## Answers

1. **A** is correct. If you enable auditing, you can track and record various security-related events, such as when someone logs on to the computer or when a file or folder is accessed. Answer B is incorrect because the access control list (ACL) is used to specify who can access an object and what permissions they have for that object. Answer C is incorrect because permissions are assigned to an object and recorded in the ACL. Answer D is incorrect because rights are used to determine what actions a user can perform on a computer running Windows.
2. **C** is correct. The first step in enabling auditing for a printer, file, or folder is that you must first enable object auditing. Printers, files, and folders are examples of objects. User auditing and ACL auditing are not specifically used in Windows audit policies and, therefore, Answers A and D are incorrect. Answer B is incorrect because configuring file auditing would be the second step after you enable object auditing.

Auditing is a feature of Windows 7 that tracks and records various security-related events so that you can detect intruders and attempts to compromise data on the system. Therefore, you want to set up an audit policy for a computer to

- ▶ Minimize the risk of unauthorized use of resources.
- ▶ Maintain a record of user and administrator activity.

Examples of auditing including tracking the success and failures of events, such as attempts to log on, attempts by a particular user to read a specific file, changes to user accounts, or changes to security settings.

Some events that you can monitor are access to an object such as a folder or file, management of user and group accounts, and logging on and off a system. The security events are provided in the Event Viewer, specifically the security logs, which contain the following information:

- ▶ The action that was performed
- ▶ The user who performed the action
- ▶ The success or failure of the event and when the event occurred
- ▶ Additional information, such as the computer where the event occurred

Therefore, auditing is one way to find security holes in your network and to ensure accountability for people's actions.

Not all events are audited by default. If you have Administrator permissions, you can specify what types of system events to audit using group policies or the local security policy (Security Settings\Local Policies\Audit Policy). In addition, Windows 7 also offers Advanced Audit Policy configuration, which allows more granular control, as shown in Figure 8.13. The amount of auditing that needs to be done depends on the needs of the organization. A minimum-security network might only audit failed logon attempts so that brute-force attacks can be detected. A high security network most likely audits both successful and failed logons to track who successfully gained access to the network.

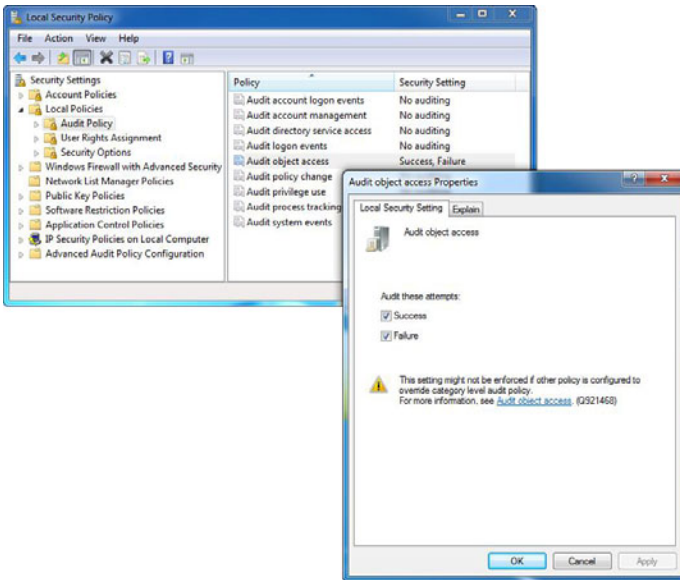


FIGURE 8.13 Auditing policy.

Auditing can be configured on any Windows computer, including workstations and servers. Because a user working on a workstation often accesses remote network resources, it makes sense that you have to configure auditing on those Windows servers so that you monitor how those resources are being accessed. In addition, because many organizations are using Active Directory domains, you need to enable auditing at the domain level so that you can monitor when a user logs in to the domain, no matter what computer they are logging from.

The first step in implementing an audit policy is to select the types of events that you want Windows 7 to audit. Table 8.3 describes the events that Windows 7 can audit.

TABLE 8.3 Audit Events

Event	Example
Account Logon	When a user logs on to the local computer, the computer records the Account Logon event. When a user logs on to a domain, the authenticating domain controller records the Account Logon event.
Account Management	An administrator creates, changes, or deletes a user account or group; a user account is renamed, disabled, or enabled; or a password is set or changed.



TABLE 8.3 Continued

Event	Example
Directory Service Access	A user accesses an Active Directory object. Note: You must then configure specific Active Directory objects for auditing.
Logon	A user logs on or off a local computer or a user makes or cancels a network connection to the computer; the event is recorded on the computer that the user accesses, regardless of whether a local account or a domain account is used.
Object Access	A user accesses a file, folder, or printer. Note: You must then configure specific files, folders, or printers to be audited, the users or groups that are being audited, and the actions that they are audited for.
Policy Change	A change is made to the user security options (for example, password options or account logon settings), user rights, or audit policies.
Privilege Use	A user exercises a user right (not related to logging on or off), such as changing the system time or taking ownership of a file.
Process Tracking	An application performs an action. This is generally used only for programmers and can be very intensive.
System	A user restarts or shuts down the computer, or an event occurs that affects Windows security or the security log.

With file and folder auditing, you can audit only those volumes that are formatted with NTFS. In addition, you must first enable Object Access auditing using group policies. After the group policy has been applied, you can set, view, or change auditing a file or folder by doing the following:

1. Using a group or local policy, enable object access auditing.
2. Open Windows Explorer and locate the file or folder that you want to audit.
3. Right-click the file or folder and select the **Properties** option.
4. Click the Security tab, click the **Advanced** button, and click the **Auditing** tab:
  - ▶ To set up auditing for a new group or user, click **Add**, specify the name of the user you want, and click the **OK** button to open the Auditing Entry box.
  - ▶ To view or change auditing for an existing group or user, click the name and then the **View/Edit** button.
  - ▶ To remove auditing for an existing group or user, click the name and then the **Remove** button.

Because the security log is limited in size, select only those objects that you need to audit and consider the amount of disk space that the security log needs. The maximum size of the security log is defined in Event Viewer by right-clicking **Security Log** and selecting the **Properties** option.

---

## Cram Quiz

1. Where do you look to see the events you audited?
  - A. System Configuration
  - B. Registry Editor
  - C. Logs folder
  - D. Event Viewer
  
2. How do you enable auditing in Windows?
  - A. Modify the boot.ini
  - B. Right-click Computer applet and select properties
  - C. Use group policies
  - D. System Configuration

## Cram Exam Answers

1. **D** is correct. If auditing is enabled, the security logs in the Event Viewer contain events. If not, the security logs are empty. Therefore, the other answers are incorrect.
  2. **C** is correct. You would enable auditing in Windows using group policies including local policies. Therefore, the other answers are incorrect.
-

## Review Questions

1. What allows a system to determine whether an authenticated user can access a resource and how they can access the resource?
  - A. Authentication
  - B. Authorization
  - C. Auditing
  - D. Certificate
2. Which protocol is the main logon authentication method used when logging onto a computer running Windows Server 2008 that is part of an Active Directory domain?
  - A. Kerberos
  - B. Windows NT LAN Manager
  - C. Certificate mappings
  - D. Password Authentication Protocol
3. Which of the following does UAC prompt for permission or administrative credentials? (Choose two answers.)
  - A. Change time zone
  - B. Change power management settings
  - C. Install fonts
  - D. Install a device driver
  - E. Install an application
4. Which of the following is used to prevent unauthorized changes to your computer?
  - A. Computer Management Console
  - B. User Account Control (UAC)
  - C. Windows Firewall
  - D. Event Viewer
5. You receive a message asking for your permission to continue a certain action. What would usually generate this warning?
  - A. Windows Firewall
  - B. NTFS permissions
  - C. User Account Control (UAC)
  - D. Internet Sharing Console

6. You work as the desktop support technician at Acme.com. You have many computers running Windows 7 that are part of a Windows domain. Your company decides to allow only applications that have been approved by the IT department. You have a handful of users who need to make configuration changes to these applications. However, when they try to make the appropriate changes, they always receive the following error message:

You need to ensure that <username> is able to make configuration changes to <computer name>.

After verifying that these users have administrative access to their computer, what do you need to do to make sure that they no longer receive these messages?

- A. Add all users to the Power Users group
  - B. Add all users to the Users group
  - C. Turn off the Windows Firewall
  - D. Change the Elevation prompt for administrators in User Account Control (UAC) Admin Approval Mode
7. You work as the desktop support technician at Acme.com. You need to assign a handful of users to install applications without giving administrative permissions. What do you do?
- A. Make these users part of the local administrator group
  - B. Turn User Account Control off in the User Accounts Control Panel tool
  - C. Configure Parental Controls to block each user from the ability to download unapproved software
  - D. Configure the User Account Control not to prompt during software installation in the Security Options section of the Local Security Policy.
8. What program do you need to download and install so that you can manage Active Directory resources from your computer running Windows 7?
- A. ADManager
  - B. WFW
  - C. UAC
  - D. RSAT
9. To create local user accounts, you use which of the following? (Choose two answers.)
- A. User Accounts in the Control Panel
  - B. Computer Management Console
  - C. Active Directory Users and Computers
  - D. Users and Groups Administrator console

10. Which auditing do you need to enable if you want to see if someone is deleting a user account from a computer running Windows 7?
- A. Account logon
  - B. Account management
  - C. Object access
  - D. Policy change

## Review Question Answers

1. Answer **B** is correct. Authorization occurs after authentication, which allows access to a network resource. Answer A is incorrect because authentication is the process to confirm a user's identity when he or she accesses a computer system or additional system resources. Answer C is incorrect because auditing is the recording of activity to be used to track user actions. Answer D is incorrect because a digital certificate is a form of authentication.
2. Answer **A** is correct. Kerberos is the main logon authentication method used by clients and servers running Microsoft Windows operating systems to authenticate both user accounts and computer accounts. Answer B is incorrect because Windows NT LAN Manager (NTLM) is an authentication protocol used for backward compatibility with pre-Windows 2000 operating systems and applications. Answer C is incorrect because certificate mappings are used with smart cards (which contain a digital certificate) for logon authentication. Answer D is incorrect because Password Authentication Protocol (PAP) is used as a remote access authentication protocol that sends username and password in clear text (unencrypted).
3. Answers **D** and **E** are correct. Installing device drivers and installing applications require administrative permission. Therefore, UAC prompts you to make sure it is something that you want done. Answers A, B, and C are incorrect because standard users can perform these actions.
4. Answer **B** is correct. User Account Control is used to prevent unauthorized changes to the computer. Answer A is incorrect because the computer management console is used to manage the computer including managing volumes, using the Event Viewer and managing local users and groups. Answer C is incorrect because the Windows firewall helps block unwanted packets from getting to your computer. Answer D is incorrect because the Event Viewer is used to look at warning and error messages and the security logs.
5. Answer **C** is correct. User Account Control asks for permission to continue when you are performing tasks that require you to be an administrator to make sure that they are tasks that you really want to complete. Answer A is incorrect because Windows Firewall prevents unwanted packets from the outside. Answer B is incorrect because NTFS permissions help protect the files on an NTFS volume. Answer D is incorrect because there is no such thing as an Internet Sharing Console.

6. Answer **D** is correct. The message is generated by User Account Control, which you can configure by using local or group policies. Answer A is incorrect because the Power Users group is left behind from Windows 2000 and XP for backward compatibility. Answer B is incorrect because all standard user accounts should already be members of the Users group. Answer C is incorrect because turning off the firewall would not get rid of the message.
7. Answer **D** is correct. You need to edit the Local Security Policy to not prompt during installs by disabling the Detect application installations and prompt for elevation setting. This allows applications to be installed without prompting for the administrative credentials. Answer A is incorrect because you don't want to give administrative permission. Answer B is incorrect because turning off User Account Control stops protecting the system. Answer C is also incorrect because Parental Controls cannot be used when a computer is connected to a domain.
8. Answer **D** is correct. Active Directory consoles including Active Directory Users and Computers console and Group Policy Management console. To install these consoles, you need to install the Microsoft Remote Server Administration Tools (RSAT) for Windows 7. Answer A is incorrect because ADManager does not exist in Windows. Answer B is incorrect because WFW is short for Windows Firewall, which is used to protect a computer from unauthorized access. Answer C is incorrect because UAC is short for User Access Control, which helps protect a computer from unauthorized changes.
9. Answer **A** and **B** are correct. The Control Panel User Accounts and the Computer Management Console, specifically under Users and Groups, are used to add and manage user accounts. Answer C is incorrect because Active Directory Users and Computers console is used to manage domain user accounts. Answer D is incorrect because the Users and Groups Administrator console does not exist.
10. Answer **B** is correct. When you enable auditing of account management, events are recorded when someone creates, changes, or deletes a user account or group; a user account is renamed, disabled, or enabled; or a password is set or changed. Answer A is incorrect because account logon auditing records when a user logs on to the local computer. Answer C is incorrect because object access auditing is the first step in monitoring access to objects, including printers, folders, and files. Answer D is incorrect because policy change audits change in local policies.

*This page intentionally left blank*

## CHAPTER 9

# Managing Files and Folders

**This chapter covers the following 70-680 Objectives:**

- ▶ Configure file and folder access
- ▶ Configure BitLocker and BitLocker To Go

The disk structure does not describe how a hard drive or floppy disk physically works, but how it stores files on the disk. In other words, it describes the formatting of the disk (file system, partitions, the root directory, and the directories). A file system is the overall structure in which files are named, stored, and organized. File systems used in Windows 7 include FAT, FAT32, and NTFS. Although FAT and FAT32 were primarily used in older operating systems, NTFS is the preferred file system in Windows 7.



# NTFS

► **Configure file and folder access**

## CramSaver

1. Which of the following file systems is the most secure and the most reliable used by Windows 7?
  - A. FAT
  - B. FAT32
  - C. NTFS
  - D. VFAT
  - E. NFS
  
2. You work as the desktop support technician at Acme.com. Pat is a member of the manager group. There is a shared folder called DATA on an NTFS partition on a remote Windows 7 computer. Pat is given the Write NTFS permission, the Manager group is giving the Read & Execute NTFS permissions, and the Everyone group has the Read NTFS permission to the DATA folder. In addition, Pat, Manager, and Everyone are assigned the shared Contributor permission to the DATA folder. When Pat logs on to the Windows 7 computer that has the DATA folder and accesses the DATA folder directly, what would be Pat's permissions? (Choose all that apply.)
  - A. Read the files in that folder
  - B. Write to the files in the folder
  - C. Execute the files in the folder
  - D. Delete the files in the folder
  - E. Have no access to the files in the folder

## Answers

1. **C** is correct. NTFS is the only one that provides security features such as encryption and NTFS permissions and the ability to use transaction tracking to keep the file system reliable. Answers A and B are incorrect because they do not offer the features just mentioned for NTFS. Answer D is incorrect because this was the name given to the FAT file system that supported long file names. NFS is a file system used in UNIX/Linux machines and is not supported by Windows 7 as a file system.
2. **A, B, C, and D** are correct. When you combine the NTFS permissions assigned to Pat and to the Manager group that Pat is a member of, Pat can read, write, execute, and delete the files in the folder. When you access a folder directly on a local computer, Share permissions do not apply.

As mentioned earlier in the book, NTFS is the preferred file system for Windows 7. It allows support for larger hard drives, has better security, including permissions and encryption, and offers disk compression and disk quotas. It is also more fault tolerant because it is a journaling file system.

## NTFS Permissions

A primary advantage of NTFS over FAT and FAT32 is that NTFS volumes have the capability to apply NTFS permissions to secure folders and files. By setting the permissions, you specify the level of access for groups and users for accessing files or directories. For example, to one user or group of users, you can specify that they can only read the file; another user or group of users can read and write to the file; and others have no access. No matter if you are logged on locally at the computer or accessing a computer through a network, NTFS permissions always apply.

The NTFS permissions that are granted are stored in an access control list (ACL) with every file or folder on an NTFS volume. The ACL contains an access control entry (ACE) for each user account and group that has been granted access for the file or folder as well as the permissions granted to each user and group. To simplify the task of administration, the NTFS permissions have been logically grouped into the standard folder and file NTFS permissions, as shown in Table 9.1. If you need finer control, you need to use special permissions. Table 9.2 shows the special permissions.

### Note

Remember that to manage your folders and files and when you open up a drive or folder, you are using Windows Explorer.

### ExamAlert

Be sure that you understand the various NTFS permissions and how they are explicitly assigned and how those permissions flow down (inherited).

TABLE 9.1 **Standard NTFS Folder and File Permissions**

Permission Level	Description
Full Control	Users can read files and folders; execute files; write, modify and delete files; change attributes of files and folders; change permissions; and take ownership of files.
Modify	Users can read files and folders, execute files, write and modify files, delete files and folders, and change attributes of files and folders.
List Folder Contents	Users can view the names of folders and subfolders in the folder. This permission is only available at the folder level and is not available at the file level.
Read & Execute	Users can see the contents of existing files and folders and can run programs in a folder.
Read	Users can see the contents of a folder and open files and folders.
Write	Users can create new files and folders and make changes to existing files and folders. Users cannot create new files or folders.

TABLE 9.2 **NTFS Folder Special Permissions**

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	✓	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permissions	✓	✓	✓	✓	✓	✓
Change Permissions	✓					
Take Ownership	✓					
Synchronize	✓	✓	✓	✓	✓	✓

**Note**

Although List Folder Contents and Read & Execute appear to have the same permissions, these permissions are inherited differently. List Folder Contents is inherited by folders but not files, and it should only appear when you view folder permissions. Read & Execute is inherited by both files and folders and is always present when you view file or folder permissions.

To set, view, change, or remove permissions on files and folders:

1. Right-click the file or folder for which you want to set permissions and click **Properties**.
2. Click the **Security** tab, as shown in Figure 9.1.

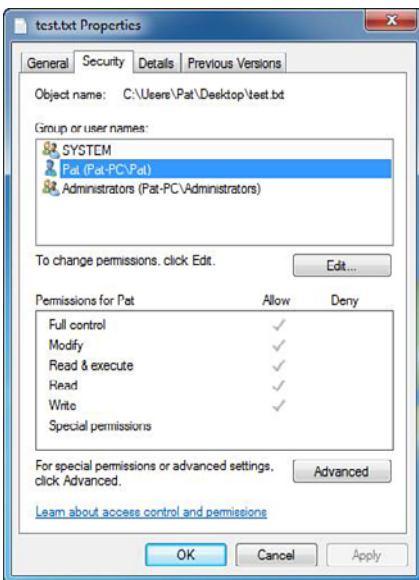


FIGURE 9.1 Properties dialog box can be used to configure NTFS permissions.

3. Click **Edit** to open the Permissions for <name of file or folder> dialog box and then do one of the following:
  - ▶ To set permissions for a group or user that does not appear in the Group or user names box, click **Add**. Type the name of the group or user you want to set permissions for and then click **OK**.

- ▶ To change or remove permissions from an existing group or user, click the name of the group or user. To allow or deny a permission, in the Permissions for <User or Group> box, select the **Allow** or **Deny** checkbox. To remove the group or user from the Group or user names box, click **Remove**.
4. To view the special permissions, click the **Advanced** button.
  5. To change the special permissions, click the **Edit** button.

When you are managing NTFS permissions, remember the following:

- ▶ You can set file and folder permissions only on drives formatted to use NTFS.
- ▶ To change permissions, you must be the owner or have been granted permission to do so by the owner.
- ▶ Groups or users that are granted Full Control for a folder can delete files and subfolders within that folder, regardless of the permissions that protect the files and subfolders.
- ▶ If the checkboxes under Permissions for <User or Group> are shaded or if the Remove button is unavailable, the file or folder has inherited permissions from the parent folder.
- ▶ When adding a new user or group, by default this user or group has Read & Execute, List Folder Contents, and Read permissions.

Permissions are given to a folder or file as either explicit permissions or inherited permissions. Explicit permissions are those granted directly to the folder or file. Some of these permissions are granted automatically, such as when a file or folder is created, while others have to be assigned manually.

When you set permissions to a folder (explicit permissions), the files and subfolders that exist in the folder inherit these permissions (called inherited permissions). In other words, the permissions flow down from the folder into the subfolders and files, indirectly giving permissions to a user or group. Inherited permissions ease the task of managing permissions and ensure consistency of permissions among the subfolders and files within the folder.

When viewing the permissions, the permissions will be checked, cleared (unchecked), or shaded. If the permission is checked, the permission was explicitly assigned to the folder or file. If the permission is clear, the user or

group does not have that permission explicitly granted to the folder or file. Note that a user may still obtain permission through a group permission or a group may still obtain permission through another group. If the checkbox is shaded, the permission was granted through inheritance from a parent folder.

Windows offers the ability to deny individual permissions. The Deny permission always overrides the permissions that have been granted, including when a user or group has been giving full control. For example, if the group has been granted read and write, yet a person has been denied the Write permission, the user's effective rights would be the Read permission.

Similar to permissions granted at a lower level, NTFS file permissions override folder permissions. Therefore, if a user has access to a file, the user is still able to gain access to a file even if he or she does not have access to the folder containing the file. Of course, because the user doesn't have access to the folder, the user cannot navigate or browse through the folder to get to the file. Therefore, a user has to use the universal naming convention (UNC) or local path to open the file.

When assigning permissions to a folder, by default, the permissions apply to the folder being assigned and the subfolders and files of the folder. If you show the permission entries, you can specify how the permissions are applied to the folder, subfolder, and files.

To stop permission from being inherited, you can select the **Replace all existing inheritable permissions on all descendants with inheritable permissions from this object** option in the Advanced Security Settings dialog box. It then asks you if you are sure. You can also clear the **Allow inheritable permissions from parent to propagate to this object** checkbox. When the checkbox is clear, Windows responds with a Security dialog box. When you click on the **Copy** button, the explicit permission is copied from the parent folder to the subfolder or file. You can then change the subfolder's or file's explicit permissions. If you click on the **Remove** button, it removes the inherited permission altogether.

Because users can be members of several groups, it is possible for them to have several sets of explicit permissions to a folder or file. When this occurs, the permissions are combined to form the effective permissions, which are the actual permissions when logging in and accessing a file or folder. They consist of explicit permissions plus any inherited permissions.

## Copying and Moving Files

When you copy and move files and folders from one location to another, you need to understand how the NTFS folder and file permissions are affected. If you copy a file or folder, the new folder and file automatically acquire the permissions of the drive or folder that the folder and file is being copied to.

If the folder or file is moved within the same volume, the folder or file retains the same permissions that were already assigned. When the folder or file is moved from one volume to another volume, the folder or file automatically acquires the permissions of the drive or folder that the file is being copied to. An easy way to remember the difference is this: When you move a folder or file from within the same volume, the folder and file are not physically moved but the Master File Table is adjusted to indicate a different folder. When you move a folder or file from one volume to another, it copies the folder or file to the new location and then deletes the old location. Therefore, the moved folder and files are new to the volume and acquire the new permissions.

### ExamAlert

When you copy a file or folder or move a file or folder to a new volume, the file or folder automatically acquires the permission and attributes (compressions and encryption) of the drive or folder that the folder and file is being copied to. If you move the file or folder to the same volume, it keeps the same permissions and attributes that it already has.

Windows Vista, Windows 7, and Windows Server 2008 also include robocopy or “Robust File Copy” to copy files and folders from one place to another (even including between computers) while keeping their NTFS permissions, attributes, and properties. Robocopy includes many parameters. For more information about these parameters, visit the following website:

[http://technet.microsoft.com/en-us/library/cc733145\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc733145(Ws.10).aspx)

## Folder and File Owners

Every folder and file has an owner, a person who controls how permissions are set on a folder or file and who grants permissions to others. When a folder or file is created, the user that creates the folder automatically becomes the owner. To be able to take ownership of a folder or file, the user has to be granted Take Ownership permission or be the administrator. After logging in, the user can take ownership by doing the following:

1. Right-click the folder or file and select the **Properties** option.
2. Click the **Security** tab and then the **Advanced** button.
3. Click the **Owner** tab.
4. Click the **Edit** button.
5. Click the user or group who is taking ownership. If the user to which you want to give ownership is not listed, you can click the **Other users or groups** button. When the user is selected, click the **OK** button.
6. When the Windows Security dialog box appears, click **OK**.
7. Click on the **OK** button to close the Advanced Properties dialog box.
8. Click **OK** to close the Properties dialog box.

## Controlling Who Can Access a USB Flash Device

By using Group Policies with Windows 7, you can block automatic installation of USB storage devices on computers, specifically by enabling the Computer Configuration\Policies\Administrative Templates\System\Devices Installation\Device Installation Restrictions\Prevent Installation of Removable Devices policy. This prevents someone from connecting a USB drive and copying sensitive data to it, assuming that the device has not already been installed prior to the group policy being applied.

---

## Cram Exam

1. You work as the desktop support technician at Acme.com. Pat is a member of the manager group. There is a shared folder called MANAGEMENT on an NTFS partition on a remote Windows 7 computer. Pat is given the Allow Write NTFS permission, the Manager group is giving the Read & Execute NTFS permissions, and the Everyone group has the Allow Read NTFS permission to the DATA folder. In addition, Pat, Manager, and Everyone are assigned the shared Contributor permission to the MANAGEMENT folder. When Pat logs on his client computer and accesses the MANAGEMENT folder, what would be Pat's permissions? (Choose all that apply.)
  - A. Read the files in that folder
  - B. Write to the files in the folder
  - C. Execute the files in the folder
  - D. Delete the files in the folder
  - E. Have no access to the files in the folder



2. You have a file, c:\data\reports.doc, on an NTFS volume. You move the file to the d:\reports folder, also on an NTFS volume. What permissions does the reports.doc receive?
- A. It retains the same permissions that it had before.
  - B. It inherits the same permissions of the c:\data\reports folder.
  - C. It inherits the same permissions of the d:\reports folder.
  - D. All permissions are removed and you as the owner are set to full control.

## Cram Exam Answers

1. **A, B, and C** are correct because NTFS permissions includes Write permission combined with Read and Execute. The Contributor share permission gives the ability to read, write, execute, and delete. When you combine the two, you take the least permissions, so that would be read, write, and execute. Answer D is incorrect because there was no delete NTFS permission assigned. Because they have permissions, Answer E is incorrect.
2. **C** is correct. If you move a file from the one NTFS volume to another NTFS volume, the file receives the same permissions as the target folder; therefore, the other answers are incorrect.
-

# Windows 7 File Structure

## ► Configure file and folder access

### CramSaver

1. You have a user called Jsmith. What is the location of JSmith's Desktop folder on the C drive?
  - A. C:\Desktop
  - B. C:\Windows\JSmith\Desktop
  - C. C:\Users\JSmith\Desktop
  - D. C:\Documents and Settings\JSmith\Desktop
2. Which of the following describes a view that enables you to aggregate information or folders from different locations?
  - A. Library
  - B. Search connector
  - C. Federation
  - D. Local index

### Answers

1. **C** is correct. The user's profile that contains the Desktop and My Documents folder is located in the C:\Users folder; therefore, the other answers are incorrect.
2. **A** is correct. A library is a new view that enables you to aggregate information from different locations. It consists of library locations. Answer B is incorrect because a search connector is an XML-based file used to search remote data stores. Answer C is incorrect because a federation provides the ability to search a remote data store, such as SharePoint. Answer D is incorrect because a local index is a component that enables a user to search his computer's content.

As you maintain and manage Windows, you need to understand how the folders and files are organized in Windows. Table 9.3 shows the most common referred folders when managing Windows. Of course, Windows is installed in the C:\Windows folder and the other programs are installed in the C:\Program Files and C:\Program Files (x86) folders.

TABLE 9.3 **Windows 7 Popular Folders**

Folder	Description
C:\Windows	The Default folder that holds the Windows operating system.
C:\Windows\System32	The C:\Windows\System32 is a folder that has many of the Windows system programs.
C:\Windows\CSC	Windows 7 store offline files in the C:\Windows\CSC folder.
C:\Windows\Fonts	The Fonts folder for Windows XP and Windows Vista. If you need to add fonts, you typically use an install program or you use the Fonts applet in the Control Panel.
C:\Windows\Logs	A place where many logs are placed.
C:\Windows\Winsxs	A folder that stores all versions of components, including DLLs, so that the system, upgrades, and rollbacks are more reliable. Over time as you install more updates (Windows and other components), this folder grows quite large. Therefore, you should make sure you leave significant free space on your C drive to avoid problems in the future.
C:\Windows\Syswow64	WoW64 stands for Windows on 64-bit Windows. It contains the 32-bit binary files required for compatibility on 64-bit Windows.
C:\Users	The Users folder has individual folders for each user who has logged into the computer. Underneath these folders, you find a Desktop, My Documents, and Start Menu folder that is mapped for each user as they logged, and these folders are combined with the Desktop, My Documents, and Start Menu of the All Users folder.
C:\Program Files	The default program to contain programs that are not part of Windows. If it is a 64-bit Windows, it contains the 64-bit programs.
C:\Program Files (x86)	The default program for x86 programs loaded on 64-bit Windows.
C:\Windows\Temp	By default, Windows uses the C:\Windows\Temp folder to store temporary files. You can sometimes manually clear this out (although some of the files might be in use) or use the disk cleanup utility.

When a user first logs onto a Windows 7 system, a profile is created under the C:\users folder. The Profile contains several folders for the user, including the Desktop folder, My Documents folder, and the Start Menu. As demonstrated in Figure 9.2, if you save a file to your desktop, it is stored in the C:\Users\\Desktop. If a file is placed in the C:\Users\All Users\Desktop folder, it appears for all users who log on to the system.

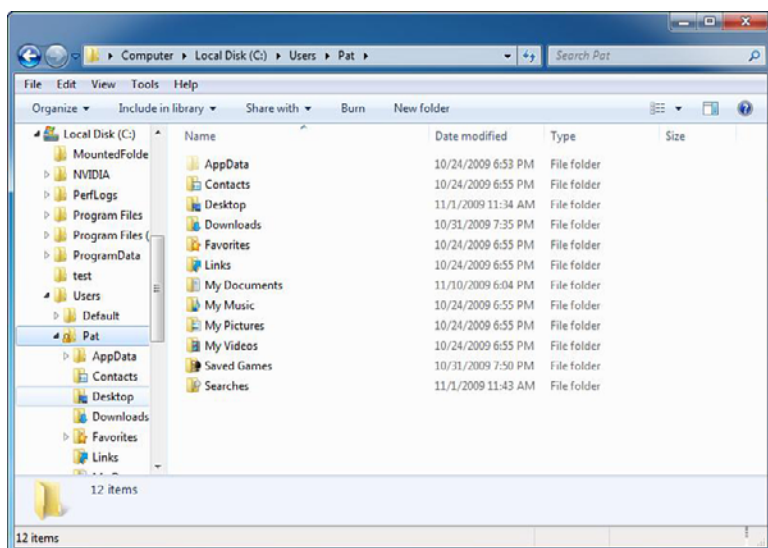


FIGURE 9.2 Profile folder structure.

## Libraries

Libraries help you view, organize, manage, and find files that are stored in different folders, on different disk drives, and on other PCs in the network. All of these locations can be combined in a library and then searched as if they are in one location. The library consists of the following components:

- ▶ **Library:** A new view that enables you to aggregate information from different locations. It consists of library locations.
- ▶ **Library location:** A component of a library that contains content—for example, a file folder, a Microsoft Office Outlook store, or a search connector.
- ▶ **Search connector:** An XML-based file used to search remote data stores.
- ▶ **Autosuggestions suggestions:** Used in a library's search box that enables building complex queries.
- ▶ **Top views:** A component that enables users to visualize the content of a library in different ways—for example, sorted by author or grouped by date.

- ▶ **Federation:** Provides the ability to search a remote data store, such as SharePoint.
- ▶ **Local search:** Search the local index, including the file system, Microsoft Office Outlook, and Microsoft Office OneNote.
- ▶ **Local index:** The component that enables users to search their computer's content.

Windows 7 includes several libraries, as shown in Figure 9.3. Of course, others can be created. The Documents library includes the My Documents folder and the Public Documents folder. The Music library includes My Music and Public Music. There is also a Pictures library and a Videos library.

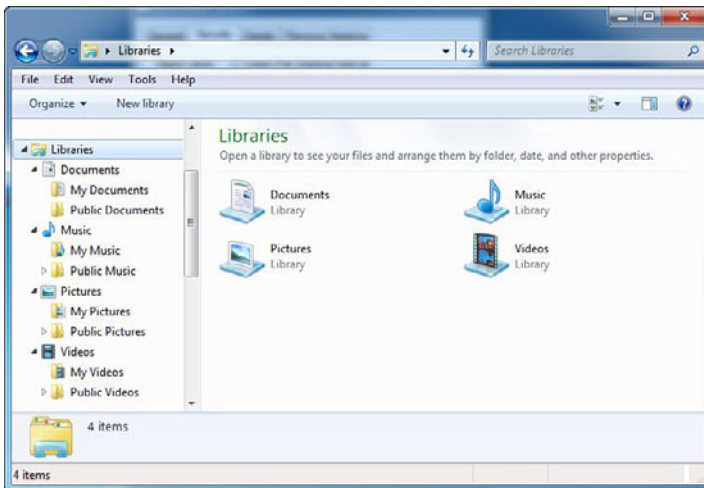


FIGURE 9.3 Default libraries.

There are two types of libraries: search-only and browse:

- ▶ **Search-only libraries:** You cannot browse them, and you must type in the search box to view any content from the library.
- ▶ **Browse libraries:** You must navigate to them to view their contents.

To make libraries faster for viewing and searching, libraries are automatically indexed. In addition, Windows 7 automatically creates libraries such as Documents, Music, Pictures, and Videos. Each library has specific top views and autosuggestions. After a suggestion is selected, a list of all the choices

(derived from the available data) appears. Users add their favorite local and remote file stores to a library in Windows 7 and one query searches across all these stores.

There are two ways to create a new library in Windows Explorer:

- ▶ Click **Libraries** in the left pane and then click **New library** on the taskbar.
- ▶ Right-click **Libraries** in the left pane, click **New**, and then click **Library**.

To share a library with another user

- ▶ Right-click the library and then click **Share with**.
- ▶ Select the library and then click **Share with** from the taskbar.

To modify an existing library, right-click the library and then click **Properties** to generate the Library properties window shown in Figure 9.4.

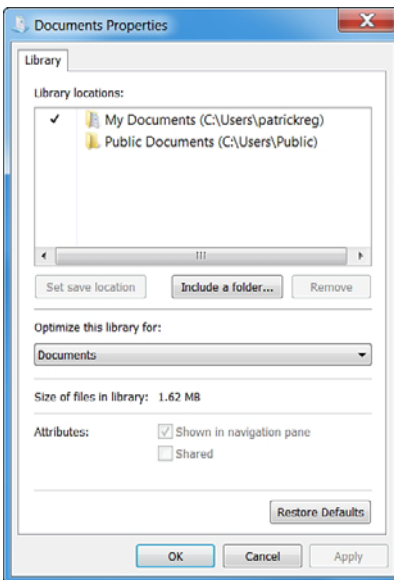


FIGURE 9.4 Library options.

## Folder Options

You can change the way files and folders function and how items are displayed on your computer by using the Folder Options in Control Panel. The Folder Options contains three tabs: General, View, and Search.

The General tab enables you to specify if each time you open a folder, it opens in the same window or in its own window. It also enables you to define how to click certain items and how to configure the navigation pane, as shown in Figure 9.5.

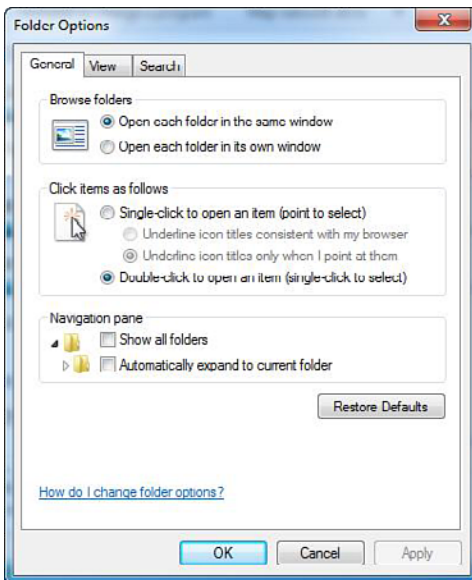


FIGURE 9.5 Folder Options General tab.

The View tab has the many advanced settings. Some of these include the following:

- ▶ Display hidden files, folders, and drives
- ▶ Hide extensions for known file types
- ▶ Hide protected operating system files
- ▶ Launch folder windows in a separate process
- ▶ Show encrypted or compressed NTFS files in color
- ▶ Use the Sharing Wizard

To restore the original settings on the View tab, click **Restore Defaults**, and then click **OK**, as shown in Figure 9.6.

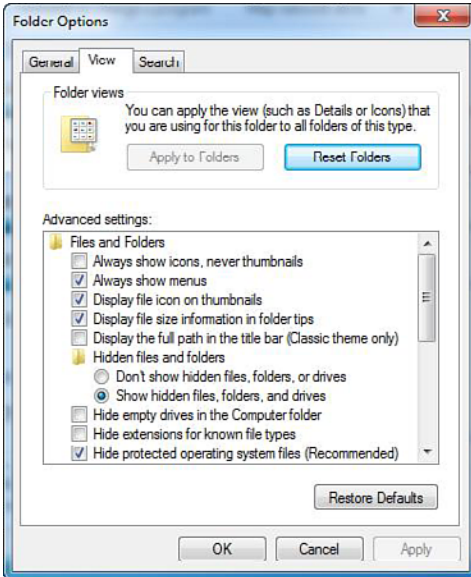


FIGURE 9.6 Folder Options View tab.

While browsing folders in the Computer folder, you can apply the current view setting to all folders on your computer that are optimized for the same content as the folder you have open. For instance, the My Pictures folder is optimized for picture files. If you open this folder and change the view to Large Icons, you can apply the Large Icons view to every folder that's optimized for pictures. (This setting does not apply when viewing files and folders using libraries.)

On the Search tab, you can configure how searches occur and what items are included in the search, including subfolders, system directories, and compressed files, as shown in Figure 9.7. You can also specify if it finds partial matches or not.



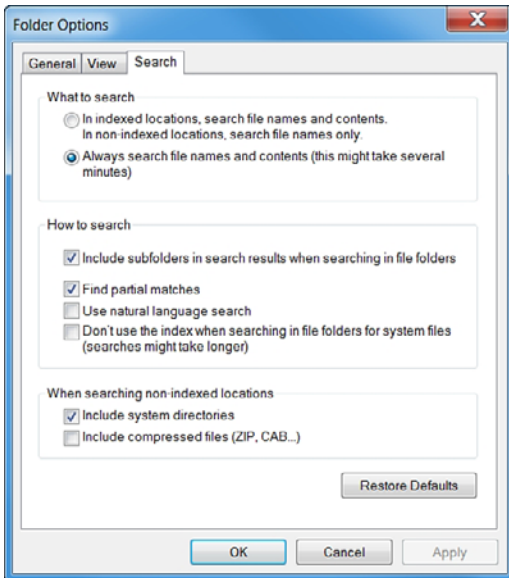


FIGURE 9.7 Folder Options Search tab.

## Searching in Windows

With larger hard drives and sometimes complicated network environments, it is more difficult to find the necessary files when you need them. Windows 7 includes the following search improvements:

- ▶ Cleaner navigation
- ▶ Arrangement views
- ▶ Instant search
- ▶ Straightforward previews
- ▶ Rich metadata
- ▶ Libraries
- ▶ Federated Search

Navigation is intuitive and optimized around storage with less overall clutter. You can now collapse nodes in the navigation pane and make it look cleaner, as demonstrated in Figure 9.8. This lack of clutter simplifies navigation in your personal files, drives, network shares, and so on.

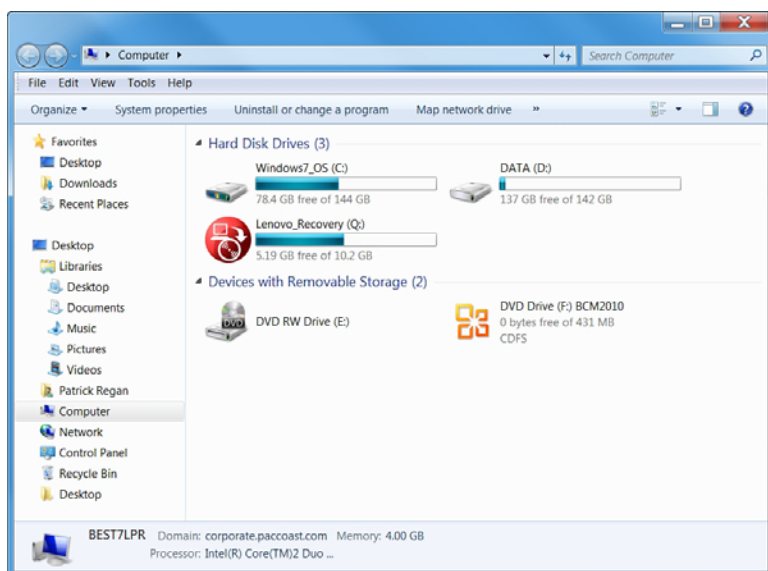


FIGURE 9.8 Windows Explorer.

At the top of a Windows Explorer window, you can configure what view you want, such as icon (Small, Medium, Large, and Extra Large), List, Tiles, and Content. You can also create folders and burn files to an optical disk.

One handy tool to help you navigate your disks and network folders is in the left pane of an open Windows Explorer window. From there, you see shortcuts to your Desktop, Downloads, Recent Places, Libraries, and Homegroup. If you scroll down a little further, you can navigate each drive using a tree structure and Network to help you navigate computers on your local network.

In addition, searching is simpler based on improved relevance, search builder, and previews. By incorporating these enhancements into Windows Explorer, libraries and Federated Search offer incredible power to search across the enterprise without learning a new user interface.

## Windows Search Tools

Windows provides several ways to find files and folders. There isn't one best way to search—you can use different methods for different situations. They include the following:

- ▶ Search box on the Start menu
- ▶ Search box located at the top of the open window
- ▶ Search box at the top of a library

You can use the Search box on the Start menu to find files, folders, programs, and email messages stored on your computer, as demonstrated in Figure 9.9. To find an item using the Start menu, click the Start button, and then type a word or part of a word in the search box. As you type, items that match your text appear on the Start menu. The search is based on text in the file name, text in the file, tags, and other file properties.

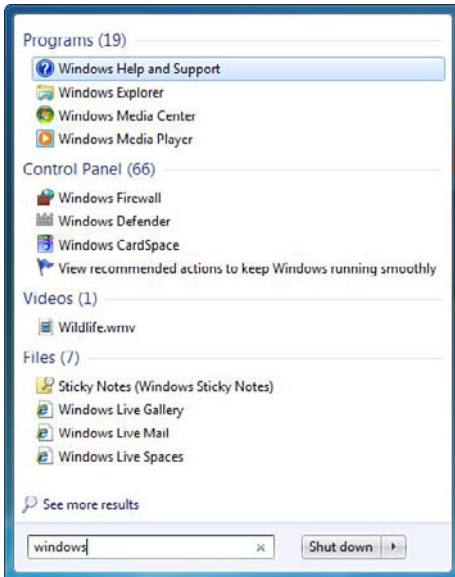


FIGURE 9.9 Search box on the Start menu.

When searching from the Start menu, only files that have been indexed appear in search results. Most files on your computer are indexed automatically. For example, anything you include in a library is automatically indexed.

You're often likely to be looking for a file that you know is in a particular folder or library, such as Documents or Pictures. Browsing for the file might mean looking through hundreds of files and subfolders. To save time and effort, use the search box at the top of the open window, as shown in Figure 9.10.

The search box is located at the top of every library. It filters the current view based on text that you type. The search looks for text in the file name and contents, and in the file properties, such as in tags. In a library, the search includes all folders included in the library as well as subfolders within those folders.

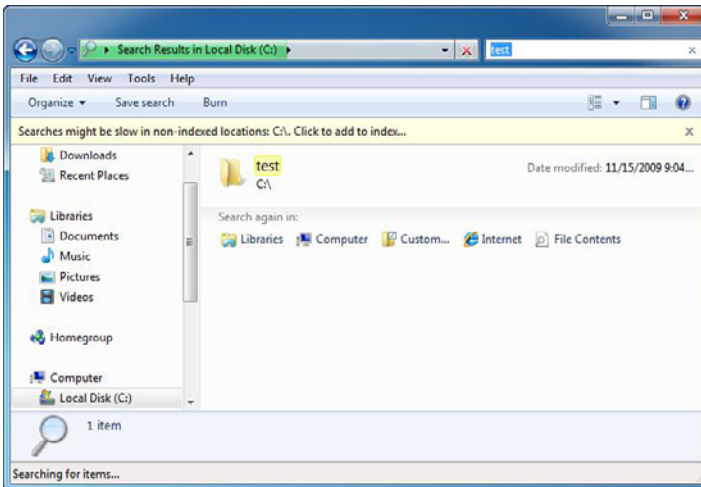


FIGURE 9.10 Search box at top of open window.

If you're searching for a file based on one or more of its properties (such as a tag or the date the file was last modified), you can use search filters to specify the property in your search.

In a library or folder, click in the search box, and then click the appropriate search filter below the search box. For example, to search the Music library for songs by a particular artist, click the Artists search filter.

Depending on which search filter you click, choose a value. For example, if you click the Artists search filter, click an artist from the list. You can repeat these steps to build complex searches on multiple properties. Each time that you click a search filter or value, terms are automatically added to the search box. If you can't find what you're looking for in a specific library or folder, you can expand the search to include different locations.

## Improving Searches Using the Index

To improve search performance, Windows uses indexes to catalog your files. By default, the commonly used files are indexed, including your libraries, email, and offline folders. Program and system files are not indexed.

If you need to add or remove index locations:

1. Click the Start menu and search for Indexing Options using the Search Programs and Files text box. Then double-click the **Indexing Options**. The Indexing options dialog box displays.

2. Click **Modify**.
3. From the resulting window shown in Figure 9.11, select to add a drive or folder or deselect a drive or folder and click **OK**.

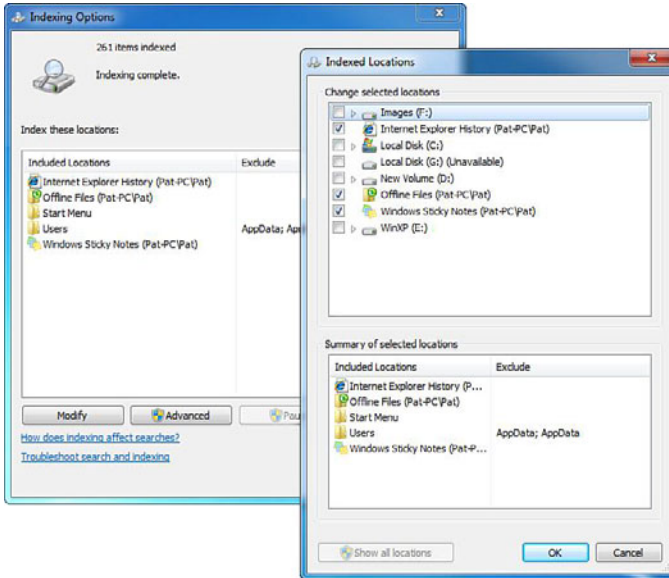


FIGURE 9.11 Changing indexing location.

If you don't see all locations on your computer in the list, click **Show all locations**. If all locations are listed, Show all locations won't be available. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

If you click the **Advanced Options**, you can rebuild your index, specify to index encrypted files, and specify where to keep the index folder and which files you want to include or not based on filename extension.

---

## Cram Exam

1. Which of the following is not a Windows 7 Search tool?
  - A. Search box on the Start menu
  - B. Search box located at the top of an open window
  - C. Indexer Search tool
  - D. Search box at the top of the library

2. Which folder would you find the 32-bit applications on a 64-bit version of Windows?
- A. C:\Program Files
  - B. C:\Program Files (x86)
  - C. C:\Windows
  - D. C:\Windows\System32

## Cram Exam Answers

1. Answer **C** is correct. The Search box on the Start menu, search box located at the top of an open window, and the search box at the top of the library are all search tools available in Windows 7. The Indexer Search tool is not. Therefore, the other answers are incorrect.
  2. Answer **B** is correct. On a 64-bit version of Windows, 32-bit applications are loaded to the C:\Program Files (x86) folder by default. Therefore, the other answers are incorrect.
-

# Encryption

- ▶ **Configure file and folder access**
- ▶ **Configure BitLocker and BitLocker To Go**

## CramSaver

1. Which of the following is not a valid requirement for BitLocker?
  - A. A computer with a TPM
  - B. A computer with only one large NTFS volume
  - C. A computer that has a compatible BIOS with TPM
  - D. A USB flash drive if your system does not have TPM
  
2. What would you use to encrypt individual files on your system?
  - A. NTFS
  - B. Compression
  - C. EFS
  - D. BitLocker

## Answers

1. **B** is correct. You need to have two NTFS volumes, not one. Answers A, C, and D are incorrect because they are requirements for BitLocker.
2. **C** is correct because EFS, which is short for Encrypted File System, is used to encrypt individual files. Answer A is incorrect because NTFS is the secure file system used in Windows that supports both compression and EFS. Answer B is incorrect because compression is used to compress files, not encrypt them. Answer D is incorrect because BitLocker is used to encrypt entire disk volumes.

If someone has administrative privilege on a Windows 7 computer or has unauthorized physical access to the device, including if the computer and/or hard drive was stolen, he or she can take ownership of files and folder, change permissions of a file, and access the file. Data can be secured against these risks by using encryption.

*Encryption* is the process of converting data into a format that cannot be read by another user. After a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. *Decryption* is the process of

converting data from encrypted format back to its original format. After a user has decrypted a file, the file remains decrypted when stored on disk.

Windows 7 offers two file encrypting technologies:

- ▶ **Encrypting File System (EFS):** EFS is used to help protect individual files on any drive on a per-user basis.
- ▶ **BitLocker Drive Encryption:** BitLocker is designed to help protect all the personal and systems files on the drive Windows is installed on if your computer is stolen or if unauthorized users try to access the computer. You can use BitLocker Drive Encryption and EFS together to get the protection offered by both features.

Table 9.3 provides a comparison of the main differences between BitLocker Drive Encryption and EFS.

**TABLE 9.3 Comparison Between Encrypting File System (EFS) and BitLocker Drive Encryption**

<b>Encrypting File System (EFS)</b>	<b>BitLocker Drive Encryption</b>
Encrypts individual files on any drive.	Encrypts all personal and system files on the drive where Windows is installed.
Encrypts files based on the user account associated with it. If a computer has multiple users or groups, each can encrypt their own files independently.	Does not depend on the individual user accounts associated with files. BitLocker is either on or off, for all users or groups.
Does not require or use any special hardware.	Uses the Trusted Platform Module (TPM), a special microchip in some newer computers that supports advanced security features.
You do not have to be an administrator to use EFS.	You must be an administrator to turn BitLocker encryption on or off after it's enabled.

## Encryption File System

Windows 7 includes the encrypting file system (EFS), which allows a user to encrypt and decrypt files that are stored on an NTFS volume. By using EFS, folders and files are kept secure against those intruders who might gain unauthorized physical access to the device, for example, as by stealing a notebook computer or a removable drive.



EFS is used to encrypt data in files and folders with a key. This key is stored in protected storage as part of your user profile, and it provides transparent access to the encrypted data.

Smart cards are supported for storing user EFS keys in addition to administrative recovery keys. If you use smart cards for logon, EFS can operate as a single sign-on service that gives transparent access to your encrypted files. The System Page file can also be protected by EFS when you configure it by using group policy.

When you are using encrypted files on a network, client-side cached copies of network files can also be encrypted, providing security for these files even if the portable computer is lost or stolen. When you use Windows in conjunction with a supported server platform, encrypted files can be transmitted over the network, and the receiving Windows client decrypts them.

### ExamAlert

EFS is only available in the Windows 7 Professional, Enterprise, and Ultimate versions. EFS is not fully supported on Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Home Premium.

To encrypt a folder or file, do the following:

1. Right-click the folder or file you want to encrypt and then click **Properties**.
2. Click the **General** tab and then click **Advanced** to generate the Advanced Attributes box, as shown in Figure 9.12.
3. Select the **Encrypt contents to secure data** checkbox and then click **OK**.

After you encrypt the file, encrypted files are colored green in Windows Explorer.

### ExamAlert

You cannot encrypt files or folders that are compressed.

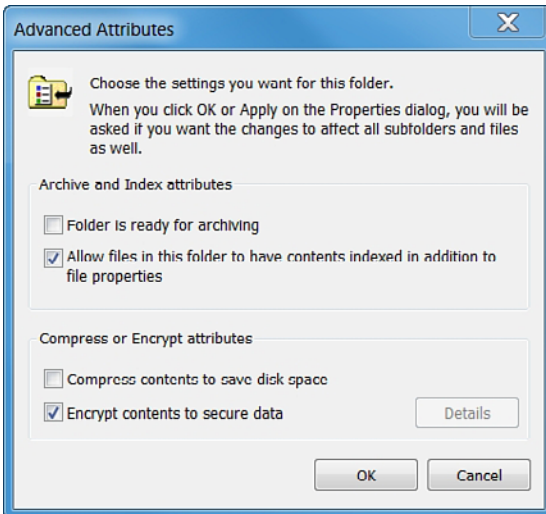


FIGURE 9.12 Encrypting a folder.

To decrypt a folder or file, use the following steps:

1. Right-click the folder or file you want to decrypt and then click **Properties**.
2. Click the **General** tab and then click **Advanced**.
3. Clear the **Encrypt contents to secure data** checkbox and then click **OK**.

## Encryption Certificates

The first time you encrypt a folder or file, you should back up your encryption certificate. If your certificate and key are lost or damaged and you do not have a backup, you won't be able to use the files that you have encrypted. To back up your EFS certificate, do the following:

1. Open Certificate Manager by clicking the Start button, typing `certmgr.msc` into the Search box, and then pressing **Enter**.
2. Click the arrow next to the Personal folder to expand it.
3. Click **Certificates**.
4. Click the certificate that lists Encrypting File System under Intended Purposes. (You might need to scroll to the right to see this.) If there is more than one EFS certificate, you should back up all of them.

5. Click the **Action** menu, point to **All Tasks**, and then click **Export**.
6. In the Export Wizard, click **Next**, click **Yes**, export the private key, and then click **Next**.
7. Click **Personal Information Exchange** and then click **Next**.
8. Type the password you want to use, confirm it, and then click **Next**. The export process creates a file to store the certificate.
9. Enter a name for the file and the location (include the whole path) or click **Browse** and navigate to the location, and then enter the file name.
10. Click **Finish**.
11. Store the backup copy of your EFS certificate in a safe place.

If the encrypted file needs to be shared with another user on the same computer, you then need to do the following:

1. Export the EFS certificate.
2. Import the EFS certificate.
3. Add the EFS certificate to the shared file.

The person with whom you want to share files needs to export her EFS certificate and give it to you by doing the following:

1. Open Certificate Manager by clicking the **Start** button, typing `certmgr.msc` into the Search box, and then pressing **Enter**.
2. Click the arrow next to the **Personal** folder to expand it and then click the EFS certificate that you want to export.
3. Click the **Action** menu, point to **All Tasks**, and then click **Export**.
4. In the Certificate Export Wizard, click **Next**.
5. Click **No**, do not export the private key, and then click **Next**.
6. On the Export File Format page, click **Next** to accept the default format.
7. The export process creates a file to store the certificate in. Type a name for the file and the location (include the whole path), or click **Browse**, navigate to the location, and then type the file name.
8. Click **Finish**.

After you get the EFS certificate from the person you want to share the file with, you need to import the certificate:

1. Open Certificate Manager by clicking the **Start** button, typing **certmgr.msc** into the Search box, and then pressing **Enter**.
2. Select the Personal folder.
3. Click the **Action** menu, point to **All Tasks**, and click **Import**.
4. In the Certificate Import Wizard, click **Next**.
5. Type the location of the file that contains the certificate, or click **Browse**, navigate to the file's location, and then click **Next**.
6. Click **Place all certificates in the following store**, click **Browse**, click **Trusted People**, and then click **Next**.
7. Click Finish.

To add the EFS certificate to the shared file, use the following steps:

1. Right-click the file you want to share and then click **Properties**.
2. Click the **General** tab and then click **Advanced**.
3. In the Advanced Attributes dialog box, click **Details**.
4. In the dialog box that appears, click **Add**.
5. In the Select User dialog box, click the certificate and then click **OK**.

## EFS Recovery Agent

To recover encrypted files with lost or damaged keys, you use a special EFS certificate. To use this special certificate, you have to create the recovery certificate, install it, and then update other EFS certificates with the recovery certificate.

To create a recovery certificate, do the following:

1. Open a command prompt.
2. Insert the removable media (a disk or USB flash drive) that you're using to store your certificate.
3. Navigate to the directory on the removable media drive where you want to store the recovery certificate by typing **drive letter** (where drive letter is the letter of the removable media) and then pressing **Enter**.

4. Type **cipher /r: filename** (where *filename* is the name that you want to give to the recovery certificate) and then press **Enter**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

Windows stores the certificate in the directory shown at the command prompt.

To install the recovery certificate, use the following steps:

1. Insert the removable media that contains your recovery certificate.
2. Click the **Start** button. In the search box, type **secpol.msc**, and then press **Enter**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the left pane, double-click **Public Key Policies**, right-click **Encrypting File System**, and then click **Add Data Recovery Agent**. This opens the Add Recovery Agent Wizard.
4. Click **Next** and then navigate to your recovery certificate.
5. Click the certificate and then click **Open**.
6. When you are asked if you want to install the certificate, click **Yes**, click **Next**, and then click **Finish**.
7. Click to open Command Prompt.
8. At the command prompt, type **gpupdate** and then press **Enter**.

To update previously encrypted files with the new recovery certificate, do the following:

1. Log on to the account you were using when you first encrypted the files.
2. Click to open Command Prompt.
3. At the command prompt, type **cipher /u** and then press **Enter**.

If you choose not to update encrypted files with the new recovery certificate at this time, the files are automatically updated the next time you open them.

## BitLocker Drive Encryption

A new feature that was added to Windows Vista was BitLocker Drive Encryption, which is designed to protect computers from attackers who have physical access to a computer. Without BitLocker Drive Encryption, an attacker

could start the computer with a boot disk and then reset the administrator password to gain full control of the computer. Or the attacker could access the computer's hard disk directly by using a different operating system to bypass file permissions.

BitLocker Drive Encryption is the feature in Windows 7 that makes use of a computer's Trusted Platform Module (TPM), which is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft than have the information stored on a USB flash drive. BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at startup, and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. BitLocker Drive Encryption also stores measurements of core operating system files in the TPM.

If a computer has a functional TPM, the encryption keys can be stored in the TPM. If someone removes the hard drive from the system, the information on the hard drive cannot be accessed because it must be decrypted with the keys stored on the TPM.

In addition, the TPM performs a hash on a snapshot of the important operating system configuration files. When the system boots, TPM performs another hash on the same system configuration files and compares the two hash values. The TPM releases the key to unlock the encrypted volume. If the values do not match, BitLocker determines that the system has been compromised, locks the drive, and goes into recovery mode. To unlock the system that is in recovery mode, you have to enter a 48-decimal-digit key. Of course, you must make sure that you create the recovery password when you turn on BitLocker for the first time. If you don't, you could permanently lose access to your files. Recovery mode is also used if a disk drive is transferred to another system.

BitLocker can be used in three ways:

- ▶ **TPM-only:** This is transparent to the user, and the user logon experience is unchanged. If the TPM is missing or changed, or if the TPM detects changes to critical operating system startup files, BitLocker enters its recovery mode, and you need a recovery password to regain access to the data.
- ▶ **TPM with startup key:** In addition to the protection provided by the TPM, a part of the encryption key is stored on a USB flash drive. This is referred to as a *startup key*. Data on the encrypted volume cannot be accessed without the startup key.

- ▶ **TPM with PIN:** In addition to the protection provided by the TPM, BitLocker requires a PIN to be entered by the user. Data on the encrypted volume cannot be accessed without entering the PIN.

By default, the BitLocker Setup Wizard is configured to work seamlessly with the TPM. An administrator can use Group Policy or a script to enable additional features and options.

On computers without a compatible TPM, BitLocker can provide encryption, but not the added security of locking keys with the TPM. In this case, the user is required to create a startup key that is stored on a USB flash drive.

On computers with a compatible TPM, BitLocker Drive Encryption can use one of two TPM modes:

- ▶ **TPM-only:** In this mode, only the TPM is used for validation. When the computer starts up, the TPM is used to validate the boot files, the operating system files, and any encrypted volumes. Because the user doesn't need to provide an additional startup key, this mode is transparent to the user and the user logon experience is unchanged. However, if the TPM is missing or the integrity of files or volumes has changed, BitLocker enters recovery mode and requires a recovery key or password to regain access to the boot volume.
- ▶ **Startup key:** In this mode, both the TPM and a startup key are used for validation. When the computer starts up, the TPM is used to validate the boot files, the operating system files, and any encrypted volumes. The user must have a startup key to log on to the computer. A startup key can be either physical, such as a USB flash drive with a machine-readable key written to it, or personal, such as a personal identification number (PIN) set by the user. If the user doesn't have the startup key or is unable to provide the correct startup key, BitLocker enters recovery mode. As before, BitLocker also enters recovery mode if the TPM is missing or the integrity of boot files or encrypted volumes has changed.

The system requirements of BitLocker are as follows:

- ▶ Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk, you must have one of the following:
  - ▶ A computer with TPM. If your computer was manufactured with TPM version 1.2 or higher, BitLocker stores its key in the TPM.

- ▶ A removable USB memory device, such as a USB flash drive. If your computer doesn't have TPM version 1.2 or higher, BitLocker stores its key on the flash drive.
- ▶ Your computer must have at least two partitions. One partition must include the drive Windows is installed on. This is the drive that BitLocker encrypts. The other partition is the active partition, which must remain unencrypted so that the computer can be started. Partitions must be formatted with the NTFS file system.
- ▶ Your computer must have a BIOS that is compatible with TPM and supports USB devices during computer startup. If this is not the case, you need to update the BIOS before using BitLocker.

To find out if your computer has TPM security hardware, do the following:

1. Open BitLocker Drive Encryption by clicking the **Start** button, clicking **Control Panel**, clicking **Security**, and then clicking **BitLocker Drive Encryption**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
2. If the TPM administration link appears in the left pane, your computer has the TPM security hardware. If this link is not present, you need a removable USB memory device to turn on BitLocker and store the BitLocker startup key that you need whenever you restart your computer.

To turn on BitLocker, follow these steps:

1. Open BitLocker Drive Encryption by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **BitLocker Drive Encryption**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
2. Click **Turn On BitLocker**. This opens the BitLocker Setup Wizard.
3. Choose how to store the recovery key:
  - ▶ Save the recovery key to a USB flash drive.
  - ▶ Save the recovery key to a file.
  - ▶ Print the recovery key.

Follow the wizard to set the location for saving or printing the recovery key. Then click **Next**.



4. When it asks if you are ready to encrypt the drive, make sure the Run BitLocker system checkbox is selected and click **Continue**.
5. When you are ready to restart the system, click the **Restart now** button.
6. While the drive is being encrypted, the Encrypting status bar is displayed, showing the progress of the drive encryption. When the drive is encrypted, a message is displayed.

To turn off or temporarily disable BitLocker, do the following:

1. Open BitLocker Drive Encryption by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **BitLocker Drive Encryption**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
2. Click **Turn Off BitLocker**. This opens the BitLocker Drive Encryption dialog box.
3. To decrypt the drive, click **Decrypt the volume**. To temporarily disable BitLocker, click **Disable BitLocker Drive Encryption**.

The BitLocker control panel applet enables you to recover the encryption key and recovery password at will. You should consider carefully how to store this information, because it allows access to the encrypted data. A domain administrator can also use group policies to automatically generate recovery passwords and back them up to Active Directory.

## BitLocker To Go

BitLocker To Go extends the BitLocker protection to removable data drives to ensure that critical data is protected when a USB drive is misplaced. You can enable BitLocker protection on a removable device by right-clicking the drive in Windows Explorer. You can also use new Group Policy settings to configure removable drives as Read-Only unless they are encrypted with BitLocker To Go.

### ExamAlert

You can use group policies to force all files copied to a removable drive to be encrypted.

When you turn on BitLocker To Go, the ensuing wizard requires that you specify how you want to unlock the drive. Select one of the following methods:

- ▶ A recovery password or passphrase
- ▶ A smart card
- ▶ Always auto-unlock this device on this PC

After the device is configured to use BitLocker, the user saves documents to the external drive. When the user inserts the USB flash drive on a different PC, the computer detects that the portable device is BitLocker protected; the user is prompted to specify the passphrase.

At this time, the user can specify to unlock this volume automatically on the second PC. It is not required that the second PC be encrypted with BitLocker. If a user forgets the passphrase, there is an option from the BitLocker Unlock Wizard—I forgot my passphrase—to assist. Clicking this option displays a recovery Password ID that can be supplied to an administrator. The administrator uses the Password ID to obtain the recovery password for the device. This Recovery Password can be stored in Active Directory and recovered with the BitLocker Recovery Password tool.

---

## Cram Quiz

1. Which technology would you use to encrypt all data on a USB flash drive?
  - A. BitLocker
  - B. BitLocker To Go
  - C. Compressed (Zipped) Folder
  - D. EFS
  
2. You right-click a file to encrypt it. You later decide to right-click the file and compress it. A few days later, you notice that the file is no longer encrypted. What is the problem?
  - A. The file is only encrypted for 72 hours.
  - B. The file was resaved in unencrypted format.
  - C. You do not have permission to encrypt the file.
  - D. You cannot have a file compressed and encrypted using NTFS at the same time.

## Cram Quiz Answers

- 1. B** is correct. BitLocker To Go extends the BitLocker protection to removable data drives to ensure that critical data is protected when a USB flash drive is misplaced. Answer A is incorrect because BitLocker is designed for hard drives. Answer C is incorrect because compression does not encrypt a drive. Answer D is incorrect because EFS could be used; however, it is designed just to encrypt individual folders and files.
  - 2. D** is correct. Because you compressed the file using NTFS, the file was automatically decrypted; therefore, the other answers are incorrect.
-

# Compression

- ▶ **Configure file and folder access**

## CramSaver

1. What are the two ways files can be compressed with Windows 7? (Choose two answers.)
  - A.** Compressed (Zipped) Folders
  - B.** EFS
  - C.** NTFS compression
  - D.** ADS

## Answers

1. **A** and **C** are correct. Compressed (Zipped) Folders is based on the same format as winzip or PKZip. If the file is on an NTFS volume, you can also go into the file or folder properties to compress the file or folder. Answer B is incorrect because EFS is used to encrypt, not compress, a file on an NTFS volume. Answer D is incorrect because Active Directory Services (ADS) is Microsoft's directory service.

Windows 7 supports two types of data compression:

- ▶ Compressed (Zipped) Folders
- ▶ NTFS compression

## Compressed (Zipped) Folders

Files and folders compressed using the Compressed (Zipped) Folders feature remain compressed under all three supported file systems: NTFS, FAT, and FAT32. Compressing any system folders, such as the \Windows folder or the \Program Files folder, is not recommended and should be avoided.

Compressed (Zipped) Folders are identified by a zipper symbol that is part of the folder's icon.

To create a Compressed (Zipped) Folder, right-click a folder, point to Send To, and click Compressed (Zipped) Folder. This action actually creates a Zip file that Windows 7 recognizes as a Compressed (Zipped) Folder that contains the folder you selected to be compressed along with all of that folder's contents.

You can also use any popular third-party utility, such as WinZip or PKZip, to read, write, add to, or remove files from any Compressed (Zipped) Folder. Unless you install such a third-party zip utility, Windows 7 displays standard zip files as Compressed (Zipped) Folders.

## NTFS Compression

NTFS compression is the ability to selectively compress the contents of individual files, entire directories, or entire drives on an NTFS volume. NTFS compression uses file compression that works by substitution. It starts by locating repetitive data with another pattern, which is shorter. Windows tracks which files and folders are compressed via a file attribute. As far as the user is concerned, the compressed drive, folder, or file is simply another drive, folder, or file that works like any other. Although you expand the amount of space for volume, the performance of the PC is slower because it has to process the compression and decompression of files. Therefore, do not use compression unless you are compressing files that are rarely used or when disk space is critical. If disk space is critical, use this as a temporary solution until you can delete or move files from the drive or can extend the volume.

To compress a file or folder on an NTFS drive, do the following:

1. Open Windows Explorer.
2. Right-click the file or folder that you want to compress and select the **Properties** option.
3. Select the **Advanced** button.
4. Select the **Compress contents to save disk space** checkbox.
5. Click on the **OK** or **Apply** button.
6. If you select to compress a drive or folder, select **Apply changes to this folder only** or **Apply changes to the folder, subfolder, and files** and click on the **OK** button.

To compress an NTFS drive, do the following:

1. Click the **Start** button entire and click **Computer**.
2. Right-click the drive that you want to compress.
3. Select the **Compress this drive to save disk space** checkbox.
4. Click the **OK** or **Apply** button.

To uncompress a drive, folder, or file, uncheck the **Compress this drive to save disk space** or **Compress drive to save disk space** box.

**ExamAlert**

You cannot compress files or folders using NTFS compression that are encrypted with EFS.

---

## Cram Quiz

1. What program do you use to manage Compressed (Zipped) or NTFS compressed files?
  - A. Internet Explorer
  - B. WinZip
  - C. Windows Explorer
  - D. zip.exe

## Cram Quiz Answer

1. **C** is correct. Windows Explorer is used to manage both compressed and NTFS compressed files. Answer A is incorrect because Internet Explorer is your web browser. Answer B is incorrect because WinZip is a third-party application that can only access the Compressed (Zipped) format. Answer D is incorrect because zip.exe does not come with Windows.
-

# Review Questions

1. You want to control the permissions of files and directories on an NTFS drive on the network. Which application must you use?
  - A. Windows Explorer
  - B. Active Directory Users and Computers console
  - C. Computer Management console
  - D. Disk Administrator console
2. Which is the minimum standard NTFS permissions needed for users to read files and folders, execute files, write and modify files, delete files and folders, and change attributes of files and folders?
  - A. Full Control
  - B. Modify
  - C. Read and Execute
  - D. Write
3. You want to modify permissions for a folder for the Everyone group; however, the permission options are grayed out. What does this mean?
  - A. You do not have sufficient permissions to change permissions.
  - B. You do not the current owner of the file.
  - C. Permissions are inherited from above.
  - D. You do not have the Take Ownership right.
4. What is the best way to prevent users from adding a USB flash drive to a Windows 7 computer?
  - A. Disable USB ports in the Device Manager
  - B. Physically disconnect the USB ports
  - C. Disable the USB ports in the BIOS
  - D. Use group policies
5. You work as the desktop support technician at Acme.com. You have configured BitLocker Drive Encryption on a computer, which has TPM installed. Unfortunately when Windows 7 starts a TPM error is displayed and the user cannot access the data on her computer because it is encrypted. What should you do?
  - A. Restart the computer and enter the recovery password at the BitLocker Driver Encryption Recovery console
  - B. Restart the computer and login as the local administrator
  - C. Disable the TPM component in the BIOS and reboot the computer
  - D. Open the TPM management console

6. You have several computers running Windows 7 connected to an Active Directory domain. You want to set up your computer with the ability to recover all EFS encrypted files on your partner's computers running Windows 7. What do you need to do?
- A. Back up the %systemroot%\DigitalLocker.
  - B. Run Secedit.exe /export on your partner's computer and run secedit.exe /import on your computer.
  - C. Run the cipher.exe /removeuser on your partner's computer. Then run cipher /adduser on your computer.
  - D. Export the data recovery agent certificate on your partner's computer and import the data recovery agent certificate on your computer.
7. You work as the desktop support technician at Acme.com. Your boss wants to protect the laptops if they get stolen. What would you do? (Choose the best answer.)
- A. Make sure that all volumes are using NTFS file system
  - B. Implement BitLocker
  - C. Implement IP Security (IPsec) for all network communications
  - D. Implement Encrypted File System (EFS) on key data files
8. What can you use to ensure that all files are encrypted if they are copied to a removable drive?
- A. Enable BitLocker To Go Drive encryption using group policies
  - B. Initialize TPM from the TPM snap-in
  - C. Enable BitLocker Drive Encryption in the Control Panel
  - D. Enable EFS on the D drive
9. What folders does the Documents library include? (Choose all that apply.)
- A. All Documents folder
  - B. My Documents
  - C. Public Documents
  - D. Favorites
10. What is used for quick searches on your hard drives?
- A. XML search file
  - B. Index
  - C. Search cache
  - D. Hash of all files



## Review Question Answers

1. Answer **A** is correct. Folders and files and their NTFS permissions are managed by the Windows Explorer. Answer B is incorrect because Active Directory Users and Computers console is used to manage the user and computer accounts within Active Directory, not NTFS permissions. Answer C is incorrect because the Computer Management console, which includes the disk administrator console, can be used to look at the event viewer, status of the disks, and manage the file system volumes but nothing with NTFS permissions. Answer D is incorrect because the disk administrator has nothing to do with NTFS permissions.
2. Answer **B** is correct. The Modify permission allows users to read files and folders, execute files, write and modify files, delete files and folders, and change attributes of files and folders. Answer A is incorrect because Full Control also gives the ability to change permissions and take ownership. Answer C is incorrect because read and Execute only allows the user to see the contents of existing files and folders and run programs. Answer D is incorrect because the write command only allows the user to create new files and folders and make changes to existing files and folders.
3. Answer **C** is correct. If the checkboxes under Permissions for <User or Group> are shaded or if the Remove button is unavailable, the file or folder has inherited permissions from the parent folder. Therefore, the other answers are incorrect.
4. Answer **D** is correct. The best way is to use group policy to prevent users access to USB flash drives, specifically the Prevent Installation of Removable Devices policy. Answers A, B, and C are incorrect because you do not want to totally disable USB, which causes other USB devices, such as mice and keyboards, to fail.
5. Answer **A** is correct. When you get a TPM error, you need to restart the computer and enter the recovery password in the recovery console. Answer B is incorrect because you cannot log in as any user because of the TPM error. Answer C is incorrect because disabling the feature in BIOS does not decrypt the disk. Answer D is incorrect because it is not able to open the TPM management console.
6. Answer **D** is correct. If you want to be able to recover files from another computer that are encrypted with EFS, you should export the data recovery agent certificate on the source computer and import the certificate to the target computer. Therefore, the other answers are incorrect.
7. Answer **B** is correct. Because BitLocker encrypts the entire drive, BitLocker is the best solution. Answer A is incorrect because you can connect a stolen hard drive to another system that has another operating system and bypass much of the security on the drive including those set by NTFS permissions. Answer C is incorrect because IPsec is used to encrypt data being transmitted over the network. Answer D is incorrect because EFS is made only to encrypt data files, not system files.

8. Answer **A** is correct. To enforce encryption, you need to enable BitLocker To Go using group policies. Answer C is incorrect. You cannot use the Control Panel because users can override the settings if they choose. Answer D is incorrect because enabling EFS does not enforce it on all removable drives. Answer B is incorrect because using the TPM snap-in does not enforce the settings.
9. Answers **B** and **C** are correct. The Documents library includes the My Documents folder and the Public Documents folder. Therefore, the other answers are incorrect.
10. Answer **B** is correct. Windows uses the index to perform very fast searches of the most common files on your computer. By default, all of the most common files on your computer are indexed. Answers A and C are incorrect because they do not exist as part of the Windows 7 operating system. Answer D is incorrect because a hash value (mathematical computation of a file) is not used for searching.

*This page intentionally left blank*

## CHAPTER 10

# Sharing Files and Folders

**This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Access to Resources:
  - ▶ Configure shared resources
  - ▶ Configure file and folder access
  - ▶ Configure BranchCache

Although many people think that Windows 7 is a workstation that requests services from other computers, typically servers, it can also act as a server to provide services. One of the traditional services that Windows 7 computers can use and provide is file sharing.

# Sharing Files and Folders

- ▶ **Configure shared resources**
- ▶ **Configure file and folder access**

## CramSaver

1. You work as the desktop support technician at Acme.com. A Windows 7 computer contains a shared folder on an NTFS partition. Which one of the following statements concerning access to the folder is correct?
  - A.** A user who is accessing the folder remotely has the same or more restrictive access permissions than if she accesses the folder locally.
  - B.** A user who is accessing the folder remotely has less restrictive access permissions than if she accesses the folder locally.
  - C.** A user who is accessing the folder remotely has the same access permissions than if she accesses the folder locally.
  - D.** A user who is accessing the folder remotely has more restrictive access permissions than if she accesses the folder locally.
  
2. You work as the desktop support technician at Acme.com. You have two users who share a computer running Windows 7 Professional Edition. Both users are working on a major report, but you don't want one user to access the other user's data files. What should you do?
  - A.** Give the appropriate NTFS permissions to both users' My Documents folders
  - B.** Have the users log in with the same account
  - C.** Instruct these users to store the report in the public folder
  - D.** Instruct these users to log out as themselves and log in as the other user to access the report
  
3. What technology was released with Windows 7 to make it easier for home users to share files and printers?
  - A.** EasyShares
  - B.** Homegroup
  - C.** UserShares
  - D.** PrivateShare

**Answers**

- 1. A** is correct. When you access a computer remotely through the share, you include the share permissions and the NTFS permissions, which can both restrict access. When you access the local folder directly, only the NTFS permissions apply. Therefore, they could have the same or more restrictive access if both are applied. Answers B and C are incorrect because if the user is accessing it remotely, the share permissions might further restrict. Answer D is incorrect because the share and NTFS permissions combined might also give the same access rather than just be more restrictive.
- 2. C** is correct. One place to store the report is in the public folder where they both can have access to it. Answers A, B, and D are not the best answers because they do not provide a secure environment where one user cannot look at the data files of another user.
- 3. B** is correct. A homegroup, new to Windows 7, makes it easier to share files and printers on a home network. You can share pictures, music, videos, documents, and printers with other people in your homegroup. EasyShares, UserShares, and PrivateShares do not exist in Windows 7. Therefore, the other answers are incorrect.

A shared folder on a computer makes the folder available for others to use on the network. A shared drive on a computer makes the entire drive available for others to use on the network. Shared drives and folders can be used on FAT, FAT32, and NTFS volumes. If used on an NTFS volume, the user still needs NTFS permissions before accessing the share.

When you share a folder with Microsoft Windows, file sharing is based on the network basic input/output system (NetBIOS) protocol and server message block (SMB). NetBIOS, which runs on top of TCP/IP, was created for IBM for its early PC networks, but it was adopted by Microsoft and has since become a de facto industry standard. It is responsible for establishing logical names (computer names) on the network, establishing a logical connection between the two computers, and supporting reliable data transfer between computers that established a session.

After a logical connection is established, computers can exchange data in the form of a NetBIOS request or in the form of a server message block. The SMB protocol, which was jointly developed by Microsoft, Intel, and IBM, allows shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network.

SMB 2.0 was introduced with Windows Vista and was used in Windows Server 2008 and Windows 7, which provided the capability to compound multiple actions into a single request, significantly reducing the number of round-trips the client needs to make to the server and improving performance as a result. Larger buffer sizes are supported, which also increases performance with large file transfers. In addition, durable file handles were introduced, which allow a connection to an SMB server to survive brief network outages, such as with a wireless network, without having to construct a new session.

When using the SMB protocol to share a directory or drive, these resources are accessed using the Universal Naming Convention (UNC):

```
\\servername\sharedname
```

The *servername* could be a NetBIOS name (computer name) or an IP address.

## Network Discovery and Browsing

With earlier versions of Windows, you could use Network Neighborhood to browse network resources such as shared folders and printers; however, this system was inefficient because it relied on network broadcasts to gather such information.

To fix this problem, Windows Vista introduced Link Layer Topology Discovery (LLTD), which queries each device that supports Plug and Play Extensions (PnP-X) or web services for devices to determine its capabilities and to determine the topology of the network. LLTD also uses version control to keep the information current. It also describes the Quality of Service (QoS) Extensions that enable stream prioritization and quality media streaming experiences, even on networks with limited bandwidth.

The information that is gathered to create the network map and which information the computer gives out to other Windows Vista, Windows 7, and Windows Server 2008 computers depends on which network services that you have enabled or configured using the Network and Sharing Center.

To enable network discovery, you need to do the following:

1. Open the **Network and Sharing Center**.
2. Click **Change advanced sharing settings**.
3. Select **Turn on network discovery**, as shown in Figure 10.1.
4. Click the **Save changes** button.

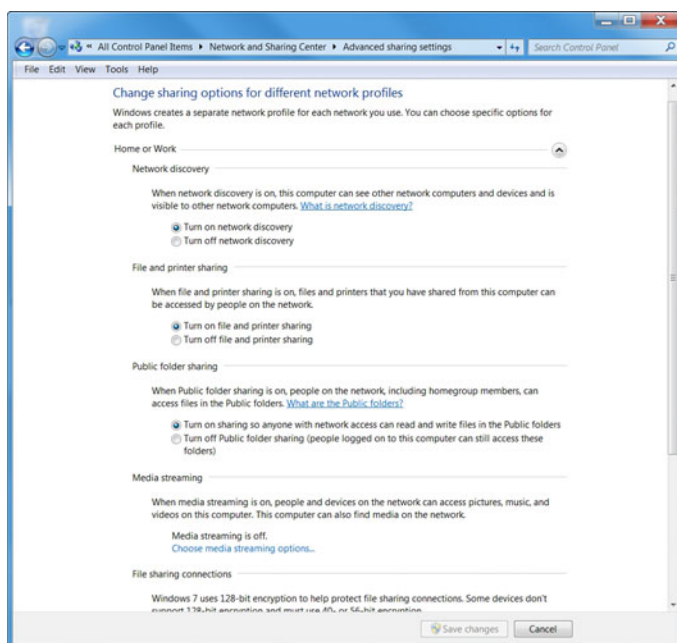


FIGURE 10.1 Managing Network Services with the Network and Sharing Center.

The network services configurable under Advanced sharing settings are as follows:

- ▶ **Network discovery:** Allows this computer to see other network computers and devices and is visible to other network computers.
- ▶ **File and printer sharing:** Files and printers that you have shared from this computer can be accessed by people on the network.
- ▶ **Public folder sharing:** People on the network can access files in the public folder.
- ▶ **Media streaming:** People and devices on the network can access pictures, music, and videos on the computer. In addition, the computer can find media on the network.
- ▶ **File-sharing connections:** Windows 7 uses 128-bit encryption to help protect file-sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.



- ▶ **Password protected sharing:** Only people who have a user account and password on the computer can access shared files, printers attached to the computer, and the public folders. To give other people access, you must turn off password protected sharing.
- ▶ **Homegroup connections:** If you have the same user accounts and passwords on all of your computers, you can choose to allow Windows to manage homegroup connections when you connect to another computer in the same homegroup. Or you can use the user account and password to connect to other computers.

Similar to Windows firewall, the network services use separate network profiles based on Home/Work and Public profiles.

To view the topology or to view the network resources, you open a network folder or the Network and Sharing Center, as shown in Figure 10.2. However, a Windows 7 computer is not visible on the network map, and it is not able to map other hardware devices on the network until you enable Network Discovery service. To see the full map, you click the View full map link in the Network and Sharing Center.

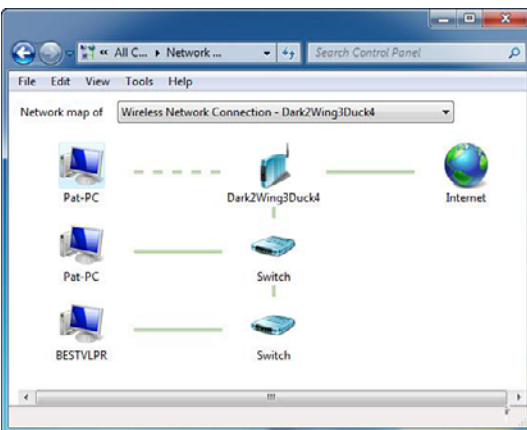


FIGURE 10.2 A sample of a network map.

### ExamAlert

LLTD is installed by default, but it only functions if you enable Network Discovery.

## Sharing Folders

In Windows 7, there are three types of sharing:

- ▶ Public sharing
- ▶ Basic sharing
- ▶ Advanced sharing

Of these three models, basic file/advanced sharing is preferred because it is more secure than public file sharing. However, public folder sharing is designed to enable users to share files and folders from a single location quickly and easily.

### Public Folders

The Public folders are handy if you want to temporarily share a document or other file with several people. It's also a handy way to keep track of what you're sharing with others; if it's in the folder, it's shared. Unfortunately, you can't restrict people to seeing just some files in the Public folder. It's all or nothing. Also, you can't fine-tune permissions. But if these aren't important considerations, then Public folders offer a convenient, alternative way to share.

Windows 7 supports the use of only one Public folder for each computer. You can copy or move any files that you want to make available publicly to an appropriate folder inside the Public folder. The Public folder is located at C:\Users\Public and contains the following subfolders, as shown in Figure 10.3:

- ▶ Public Documents
- ▶ Public Downloads
- ▶ Public Music
- ▶ Public Pictures
- ▶ Public Recorded TV
- ▶ Public Videos

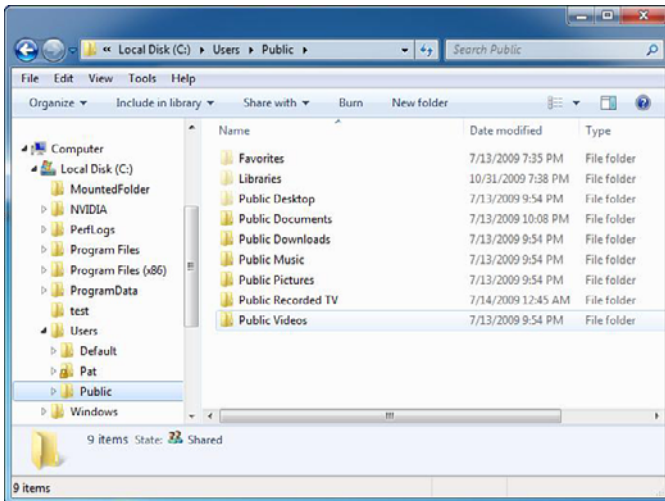


FIGURE 10.3 Public folders.

Another folder worth mentioning is the Public Desktop folder, which is used for shared desktop items. Any files and program shortcuts placed in the Public Desktop folder appear on the desktop of all users who log on to the computer (and to all network users if network access has been granted to the Public folder).

For Windows 7, public folder sharing is disabled by default. By default, files stored in the Public folder hierarchy are available to all users who have an account on this computer and can log on to it locally. You cannot access the Public folder from the network. To enable and configure public folder sharing, you need to enable the public folder sharing service using Network and Sharing Center.

Public folder sharing is turned off by default, except on a homegroup (homegroups are discussed later in this chapter). To access public folders using Windows Explorer, access the Documents library, Music library, Picture library, or Video library. You can also access the public user folders at `c:\users\public`.

Public folder sharing settings are set on a per-computer basis. If you want to share a file, you just need to copy or move the file into the `C:\Users\Public` folder. When the file is copied or moved to the Public folder, access permissions are changed to match that of the Public folder so that all users who log on to the computer and all network users that has been granted access to the Public folder can access the file.

## Basic Sharing

Creating and managing a shared folder is a little bit more of a manual process than the public sharing model, but it enables you to share any folder on the Windows 7 computer, and it gives you more fine-tuned control over sharing the folders.

Basic file sharing enables you to use a standard set of permissions to allow or deny initial access to files and folders over the network. Basic file-sharing settings are enabled or disabled on a per-computer basis. To enable File Sharing, you have to do the following:

1. Open the **Network and Sharing Center**.
2. Click the **Change advanced sharing settings**.
3. To enable file sharing, select **Turn on file and printer sharing**. To disable file sharing, select **Turn off file and printer sharing**.
4. Click **Save changes**.

There are two ways to share a folder. The first (and quickest) way is to right-click the folder you want to share and click **Share with**, as shown in Figure 10.4. You can also click the **Share with** button at the top of the Windows Explorer window. Then, select who you want to share the folder with. Your choices are Nobody, Homegroup (Read), Homegroup (Read/Write), and Specific people. If you select Specific people, you can give Read access or Read/Write access, as shown in Figure 10.5.

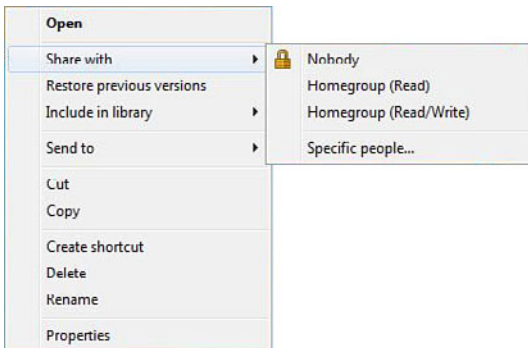


FIGURE 10.4 Share with options.

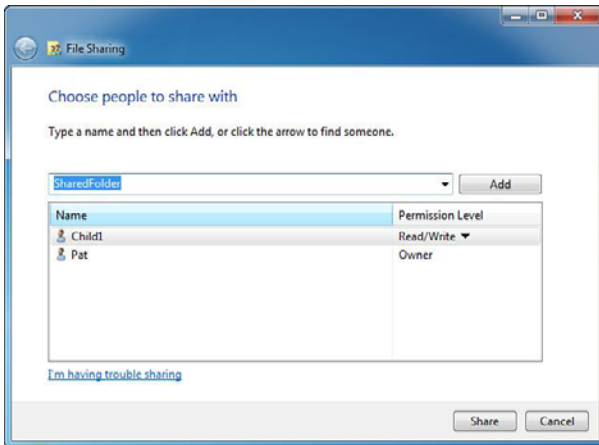


FIGURE 10.5 Specifying people to access a share and their permissions levels.

You can also right-click a folder and select Properties to display the window shown in Figure 10.6. If you click the **Share** button, you can share a folder similar to selecting specific people using a wizard.

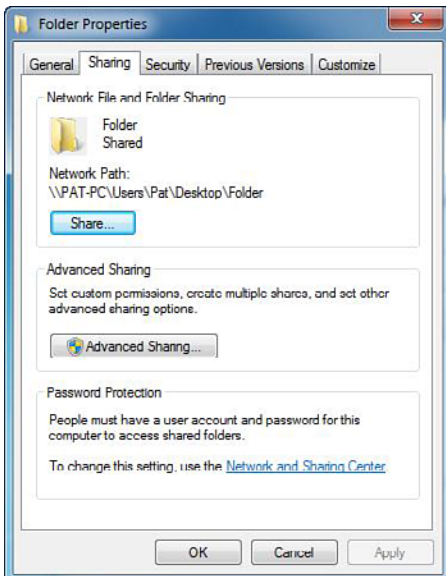


FIGURE 10.6 Folder Properties Sharing tab.

## Advanced Sharing

If you click **Advanced Sharing**, you can specify the name of the shared folder. A shared folder can be shared several times with different share names and permissions. To configure the permissions for the Shared folder, click the **Permissions** button (see Figure 10.7).

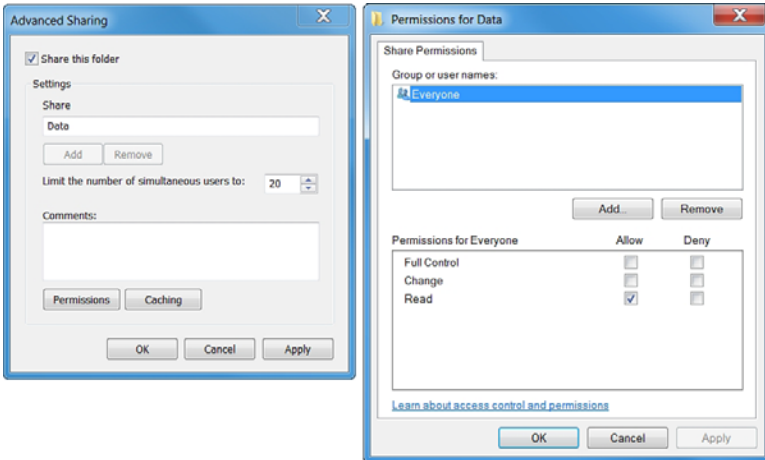


FIGURE 10.7 Advanced Sharing.

When a user accesses a file or folder in a Share over the network, the two levels of permissions are user: share permissions and NTFS permissions (if it is on an NTFS volume). The three share permissions are as follows:

- ▶ **Full Control:** Users allowed this permission have Read and Change permissions, as well as the additional capabilities to change file and folder permissions and take ownership of files and folders. If you have Owner/Co-owner permissions on a shared resource, you have full access to the shared resource.
- ▶ **Change:** Users allowed this permission have Read permissions and the additional capability to create files and subfolders, modify files, change attributes on files and subfolders, and delete files and subfolders. If you have Change permissions on a shared resource, the most you can do is perform read operations and change operations.
- ▶ **Read:** Users with this permission can view file and subfolder names, access the subfolders of the share, read file data and attributes, and run program files. If you have Read permissions on a shared resource, the most you can do is perform read operations.

**ExamAlert**

If the user accesses the computer directly where the share folder is located and accesses the folder directly without going through the share, share permissions do not apply.

Because a user can be a member of several groups, it is possible for the user to have several sets of permissions to a shared drive or folder. The effective permissions are the combination of all user and group permissions. For example, if a user has the Change permissions to the user and a Read permission to the group, of which the user is a member, the effective permissions are the Change permissions. Like NTFS permissions, Deny permissions override the granted permission.

To create a shared folder using the shared folder model is a multipart process:

1. Share the folder so that it can be accessed.
2. Set the share permissions.
3. Check and modify the NTFS file system permissions.

When accessing a shared folder on an NTFS volume, the effective permissions that a person can have in the share folder are calculated by combining the shared folder permissions with the NTFS permissions. When combining the two, first determine the cumulative NTFS permissions and the cumulative shared permissions and apply the more restrictive permissions—the one that gives the least permission.

**ExamAlert**

When figuring out the overall access a person has, combine the NTFS permissions and determine the cumulative NTFS permissions. Then determine the cumulative shared permissions and apply the more restrictive permissions between the NTFS and shared permission. Don't forget that deny permissions supersede all others.

## Special and Administrative Shares

In Windows 7, there are several special shared folders that are automatically created by Windows for administrative and system use, as described in Table 10.1. Different from regular shares, these shares do not show when a user

browses the computer resources using My Network Places, Network, or similar software. In most cases, special shared folders should not be deleted or modified. For Windows 7 computers, only members of the Administrators, Backup Operators, and Server Operators group can connect to these shares.

**Table 10.1 Special Shares**

Special Share	Description
Drive letter\$	A shared folder that allows administrative personnel to connect to the root directory of a drive, also known as an administrative share. It is shown as A\$, B\$, C\$, D\$, and so on. For example, C\$ is a shared folder name by which drive C might be accessed by an administrator over the network.
ADMIN\$	A resource used by the system during remote administration of a computer. The path of this resource is always the path to the Windows system root (the directory in which Windows is installed: for example, C:\Windows).
IPC\$	A resource sharing the named pipes that are essential for communication between programs. It is used during remote administration of a computer and when viewing a computer's shared resources.
PRINT\$	A resource used during remote administration of printers.
FAX\$	A shared folder on a server used by fax clients in the process of sending a fax. The shared folder is used to temporarily cache files and access cover pages stored on the server.

An administrative share is a shared folder typically used for administrative purposes. To make a shared folder or drive into an administrative share, the share name must have a \$ at the end of it. Because you cannot see the share folder or drive during browsing, you have to use a UNC name, which includes the share name (including the \$). Instead, you have to access it by using the **Start** button, selecting the **Run** option, and typing the UNC name and clicking the **OK** button. By default, all volumes with drive letters automatically have administrative shares (C\$, D\$, E\$, and so on). You can create other administrative shares as needed for individual folders.

## Homegroup

A homegroup, new to Windows 7, makes it easier to share files and printers on a home network. You can share pictures, music, videos, documents, and printers with other people in your homegroup. Other people can't change the files that you share, unless you give them permission to do so. When you set up a computer with Windows 7, a homegroup is created automatically if one doesn't already exist on your home network. If a homegroup already exists,



you can join it. After you create or join a homegroup, you can select the libraries that you want to share. You can prevent specific files or folders from being shared, and you can share additional libraries later. You can help protect your homegroup with a password, which you can change at any time.

### ExamAlert

Homegroups are only available with Windows 7. You can join a homegroup in any edition of Windows 7, but you can only create one in Home Premium, Professional, or Ultimate.

To join a homegroup, your computer's network location must be set to Home. To change a network location, do the following:

1. Open the **Network and Sharing Center**.
2. Click **Work network**, **Home network**, or **Public network** to open the Set Network Location dialog box, as shown in Figure 10.8, and then click the network location you want: **Home network**, **Work network**, or **Public network**.

Computers that belong to a domain can join a homegroup, but they can't share files with the homegroup. They can only access files shared by others.

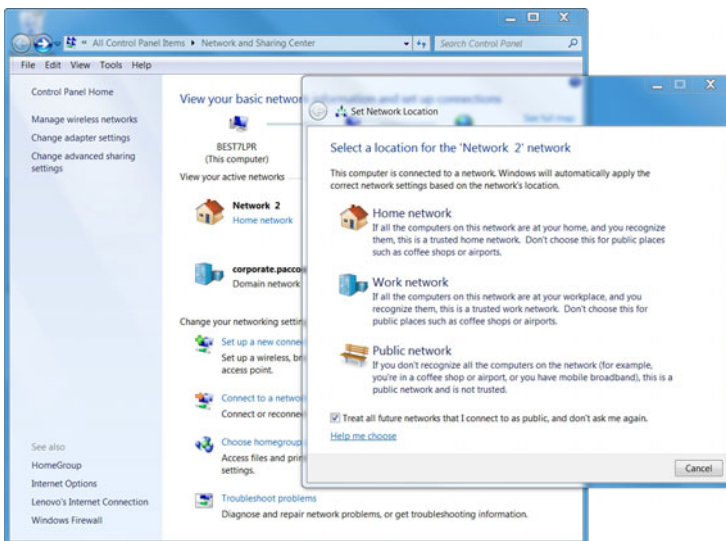


FIGURE 10.8 Selecting a network location.

After someone on your network creates a homegroup, the next step is to join it. You need the homegroup password, which you can get from the person who created the homegroup. When you join a homegroup, all user accounts on your computer become members of the homegroup. To join a homegroup, follow these steps on the computer that you want to add to the homegroup:

1. Click to open Homegroup.
2. Click **Join now** and then complete the wizard.

If you don't see the Join now button, there might not be a homegroup available. Make sure that someone has created a homegroup first. Or you can choose to create a homegroup yourself.

To create a homegroup, follow these steps:

1. Open the Control Panel and click **Choose homegroup and sharing options**.
2. On the Share with other home computers running Windows 7 page, click a homegroup to start the wizard.

To remove a computer from a homegroup, follow these steps on the computer you want to remove:

1. Open the Control Panel and click **Choose homegroup and sharing options**.
2. Click **Leave the homegroup**.
3. Click **Leave the homegroup**, and then click **Finish**.

If everyone leaves the homegroup, it no longer exists.

If your computer is part of a homegroup, you can change settings by following these steps:

1. Open the Control Panel and click **Choose homegroup and sharing options**.
2. Select the settings you want (see Table 10.2) and then click **Save changes**.

TABLE 10.2 **Homegroup Options**

Option	Description
Share libraries and printers	Select the libraries and printers you want to share in their entirety with your homegroup.
Share media with devices	Use this setting to share media with all devices on your network. For example, you can share pictures with an electronic picture frame, or share music with a network media player. Unfortunately, shared media is not secure. Anyone connected to your network can receive your shared media.
View or print the homegroup password	View or print the password for your homegroup.
Change the password	Change the password for your homegroup.
Leave the homegroup	Leave your homegroup.
Change advanced sharing settings	Change settings for network discovery, file sharing, public folder sharing, password-protected sharing, homegroup connections, and file-sharing connections.
Start the Homegroup troubleshooter	Troubleshoot homegroup problems.

To prevent a library from being shared (*while* creating or joining a homegroup), follow these steps:

1. Open the **Network and Sharing Center**.
2. Click **Choose homegroup and sharing options**.
3. Do one of the following:
  - ▶ To create a new homegroup, click **Create a homegroup**.
  - ▶ To join an existing homegroup, click **Join now**.
4. On the next screen of the wizard, clear the checkbox for each library you don't want shared. The Create a Homegroup dialog box appears.
5. Click **Next**, and then click **Finish**.

To prevent a library from being shared (*after* creating or joining a homegroup), do the following:

1. Click to open Homegroup.
2. Clear the checkbox for each library you don't want shared and then click **Save changes**.

To prevent specific files or folders from being shared (after creating or joining a homegroup), follow these steps:

1. Click the **Start** button and then click your user name.
2. Navigate to the file or folder you want to exclude from sharing and then select it.
3. Do one of the following:
  - ▶ To prevent the file or folder from being shared with anyone, in the toolbar, click **Share with**, and then click **Nobody**.
  - ▶ To share the file or folder with some people but not others, in the toolbar, click **Share with**, click **Specific people**, select each person you want to share with, and then click **Add**. Click **Share** when you are finished.
  - ▶ To change the level of access to a file or folder, in the toolbar, click **Share with** and then select either **Homegroup (Read)** or **Homegroup (Read/Write)**.

## Managing Shares

By using the Shared Folders snap-in (included in the Computer Management Console), you can manage the server's shared folders. With the Shared Folder snap-in, you can do the following:

- ▶ Create, view, and set permissions for shares, including shares on Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008
- ▶ View a list of all users who are connected to the computer over a network and disconnect one or all of them
- ▶ View a list of files opened by remote users and close one or all of the open files

## Connecting to a Shared Folder

After you share a file or folder, users can connect to it as a network resource or map to it by using a drive letter on their machines. After a network drive is mapped, users can access it just as they would a local drive on their computer.

You can map a network drive to a shared file or folder by completing the following steps:

1. Click **Start** and then click **Computer**.
2. In Windows Explorer, click the **Map Network Drive** button on the toolbar. This displays the Map Network Drive dialog box, as shown in Figure 10.9.
3. Use the Drive field to select a free drive letter to use and then click the Browse button to the right of the Folder field.
4. In the Browse for Folder dialog box, expand the Network folders until you can select the name of the workgroup or the domain with which you want to work. When you expand the name of a computer in a workgroup or a domain, you see a list of shared folders. Select the shared folder you want to work with and then click **OK**.
5. Select **Reconnect at logon** if you want Windows 7 to connect to the shared folder automatically at the start of each session.
6. If your current logon doesn't have appropriate access permissions for the share, click the **Different User Name** link. You can then enter the user name and password of the account with which you want to connect to the shared folder. Typically, this feature is used by administrators who log on to their computers with a limited account and also have an administrator account for managing the network.
7. Click **Finish**.

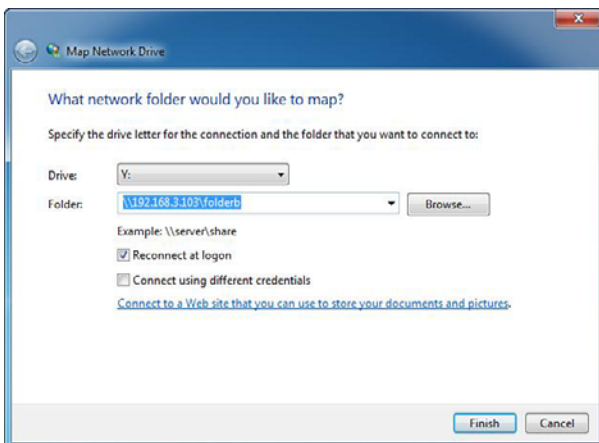


Figure 10.9 The Map Network Drive dialog box.

If you later decide you don't want to map the network drive, click **Start** and then click **Computer**. In Windows Explorer, under Computer in the right pane, right-click the network drive icon and choose **Disconnect**.

You can also type in a UNC in the Search program and files box, a Run box, or the address bar in Windows Explorer. To display the Run box quickly, use the Windows logo key + R shortcut. If you don't have a Windows logo key or if you prefer to use the mouse, you can add the Run option to the Start menu in Windows 7:

1. Right-click the Start button and choose **Properties**.
2. On the Start Menu tab, click the **Customize** button to the right of the Start Menu option.
3. In the Customize Start Menu dialog box, scroll down and place a checkmark next to the **Run** command.
4. Click **OK** to save your changes.

---

## Cram Quiz

1. What type of share is not displayed when browsed using Network?
  - A. Public share
  - B. Hidden share
  - C. Administrative shares
  - D. NTFS share
2. Which editions of Windows 7 allow you to create a homegroup? (Choose all that apply.)
  - A. Home Basic
  - B. Home Premium
  - C. Professional
  - D. Ultimate

3. You have shared a couple of folders on your Windows 7 computer. Unfortunately, they are not visible on anyone's network map so that users can find the shares easily. What is most likely the problem?
- A. You need to enable the Network Discovery service.
  - B. You did not give the appropriate share permissions to the Everyone group.
  - C. You did not give the appropriate NTFS permission to the Everyone group.
  - D. You need to make sure there is a DNS entry in the DNS server for the Windows 7 computer.

## Cram Quiz Answers

1. **C** is correct. Different from regular shares, these shares do not show when a user browses the computer resources using Network, My Network Place, or similar software. The public share, hidden share, and NTFS are not types of shares. Therefore, the other answers are incorrect.
  2. **B, C, and D** are correct. You can join a homegroup in any edition of Windows 7, but you can only create one in Home Premium, Professional, or Ultimate; therefore, Answer A (Home Basic) is incorrect.
  3. **A** is correct. To view the computer using the network map, you need to have the Link Layer Topology Discovery (LLTD) operational. Therefore, you need to enable the Network Discovery service. Answers B and C are incorrect because Share and NTFS permissions have nothing to do with a computer showing on the network map. Answer D is incorrect because there is no indication that there is a name resolution problem.
-

# BranchCache

## ► Configure BranchCache

### CramSaver

1. What technology is designed to reduce traffic (including web and file sharing traffic) between two remote sites, specifically between the central site and a smaller remote site?
  - A. Distributed File System
  - B. ProxyServer
  - C. IIS
  - D. BranchCache

### Answer

1. Answer **D** is correct. BranchCache caches files on a remote site after it communicates with the central office so that in the future, it can use the cache to provide files without always going to the central office. As a result, BranchCache reduces traffic. Answer A is incorrect because Distributed File System (DFS) is used to group shares together or to create redundancy among shared folders. Answer B is incorrect because the Proxy Server is used to cache web pages. Answer C is incorrect because IIS, short for Internet Information Service, is used to provide web services.

Branch offices are often connected to enterprises with a low-bandwidth link. Therefore, accessing corporate data located in the enterprise is slow. BranchCache helps to resolve these challenges by caching content from remote file and web servers so that users in branch offices can access corporate information more quickly. The cache can be hosted centrally on a server (such as a Windows Server 2008 R2) in the branch location, or it can be distributed across user computers.

If the cache is distributed, the branch users' computer automatically checks the cache pool to determine if the data has already been cached. If the cache is hosted on a server, the branch users' computer checks the branch server to access data. Each time a user tries to access a file, his or her access rights are authenticated against the server in the data center to ensure that the user has access to the file and is accessing the latest version.



In the distributed caching mode, cache is distributed across client computers in the branch. Using this type of peer-to-peer architecture, content is cached on Windows 7 clients after it is retrieved from a Windows Server 2008 R2. Then it is sent directly to other Windows 7 clients as they need it.

When you use the hosted caching mode, cache resides on a Windows Server 2008 R2 computer that is deployed in the branch office. Using this type of client/server architecture, Windows 7 clients copy content to a local computer (Hosted Cache) running Windows Server 2008 R2 that has BranchCache enabled.

Compared to Distributed Cache, Hosted Cache increases cache availability because content is available even when the client that originally requested the data is offline. A computer must obtain the identifier that describes a piece of content to decrypt that content after downloading. The identifiers, provided by the server, include a digest of the content. After downloading from the cache, the client computer verifies that the content matches the digest in the identifier. If a client downloads an identifier from the server but cannot find the data cached on any computers in the branch, the client returns to the server for a full download.

BranchCache caches content for the most common protocols including HTTP, HTTPS, and SMB, and it supports network security protocols SSL and IPsec. On Windows 7 clients, BranchCache is off by default. Client configurations can be performed through Group Policy or it can be done manually.

BranchCache is disabled by default on client computers. Take the following steps to enable BranchCache on client computers:

1. Turn on BranchCache.
2. Enable either Distributed Cache mode or Hosted Cache mode.
3. Configure the client firewall to enable BranchCache protocols.

Most of these steps are done with Windows Server 2008 R2 domain controllers and group policies. You then need to configure the Windows 7 computers using group policies and make sure that the BranchCache service is started.

---

## Cram Quiz

1. Which mode of BranchCache has the cached data reside on local clients at a remote site?
  - A. Distributed Cache
  - B. Hosted Cache
  - C. Proxy Cache
  - D. Link Cache

## Cram Quiz Answers

1. **A** is correct because Distributed Cache is distributed across Windows 7 client computers in the branch. Answer B is incorrect because when you use the hosted caching mode, cache resides on a Windows Server 2008 R2 computer that is deployed in the branch office. Answers C and D are incorrect because they are not types of cache used in the BranchCache.
-

## Review Questions

1. What is the minimum share permission that allows you to read and execute files, create files and subfolders, modify files, and change attributes?
  - A. Full Control
  - B. Change
  - C. Write
  - D. Read
2. You have a shared folder on an NTFS volume. What is the best way to share the folder and lock it down?
  - A. Set Everyone to have full control share permission and lock it down with NTFS permission
  - B. Set Everyone to have full control NTFS permissions and lock it down with share permissions
  - C. Set Everyone to have full control NTFS and share permissions and lock it down with file attributes
  - D. Lock it down with both share and NTFS permissions
3. You work as the desktop support technician at Acme.com. Pat is a member of the manager group. There is a shared folder called DATA on an NTFS partition on a remote Windows 7 computer. Pat is given the Write NTFS permission, the Manager group is giving the Read & Execute NTFS permissions, and the Everyone group has the Read NTFS permission to the DATA folder. In addition, Pat, Manager, and Everyone are assigned the shared Reader permission to the DATA folder. When Pat logs on his client computer and accesses the DATA folder, what would be Pat's permissions? (Choose all that apply.)
  - A. Read the files in that folder
  - B. Write to the files in the folder
  - C. Execute the files in the folder
  - D. Delete the files in the folder
  - E. Have no access to the files in the folder.
4. You work as the desktop support technician at Acme.com. Pat is a member of the manager group. There is a shared folder called DATA on an NTFS partition on a remote Windows 7 computer. Pat is given the Write NTFS permission, the Manager group is giving the Deny All NTFS permissions and the Everyone group has the Read NTFS permission to the DATA folder. In addition, Pat, Manager, and Everyone are assigned the shared Contributor permission to the DATA folder. When Pat logs on his client computer and accesses the DATA folder, what would be Pat's permissions? (Choose all that apply.)

- A. Read the files in that folder
  - B. Write to the files in the folder
  - C. Execute the files in the folder
  - D. Delete the files in the folder
  - E. Have no access to the files in the folder
5. Which type of sharing is designed to enable users to share files and folders from a single location quickly and easily?
- A. Public sharing
  - B. Basic sharing
  - C. Advanced sharing
  - D. Password sharing
6. Where would you enable network discovery?
- A. Network and Sharing Center
  - B. Services console
  - C. Shared console
  - D. Network console
7. You need to access the C:\Data folder on your partner's computer. Unfortunately, he did not share the folder. If you are an administrator on his computer, how can you access the Data folder remotely?
- A. Open the C:\Data folder
  - B. Open the \\Computername\C\Data folder
  - C. Open the \\Computername\C\$\Data folder
  - D. Open the \\Computername\C:\Data folder
8. Where does the Public shared folder reside?
- A. C:\Public
  - B. C:\Users\Public
  - C. C:\Windows\Public
  - D. C:\Shares\Public
9. Which special or administrative share is used during remote administration of a computer and for viewing a computer's shared resources?
- A. NetLogin
  - B. PRINT\$
  - C. C\$
  - D. IPC\$

10. Which mode of BranchCache has the cached data reside on a Windows Server 2008 R2 server?
- A. Distributed Cache
  - B. Hosted Cache
  - C. Proxy Cache
  - D. Link Cache

## Review Question Answers

1. Answer **B** is correct. The Change permission allows you to read files, create files and subfolders, modify files, change attributes on files and subfolders, and delete files and subfolders. Answer A is incorrect because the Full Control permission also allows you to change permissions. Answer C is incorrect because the Write share permission does not exist. Answer D is incorrect because the Read permission does not give you write capability.
2. Answer **A** is correct. With Microsoft's best practices, you should grant full control to Everyone and use NTFS to lock it down. Answer B is incorrect because setting full control NTFS permissions to everyone does not control users who access the folder locally. Answer C is incorrect because you cannot secure files and folders with attributes. Answer D is incorrect because while you could lock down the folder with share and NTFS permissions, it is simpler to control through one mechanism instead of two.
3. Answers **A** and **C** are correct. When you combine the NTFS permissions assigned to Pat and to the Manager group that Pat is a member of, Pat can read, write, execute, and delete the files in the folder. However, because the Reader share permission only allows reading and executing the files, blocking writing, and deleting when going through the shared folder. Answers B and D are incorrect because the Reader permission blocks the Write and Delete permissions.
4. Answer **E** is correct. Pat is a member of the Managers group. Because Deny All NTFS permissions has been granted to the Managers group, it blocks all permissions for Pat. Answers A, B, C, and D are incorrect because no access permissions always wins.
5. Answer **A** is correct. Public folder sharing is designed to enable users to share files and folders from a single location quickly and easily. The Public folders are handy if you want to temporarily share a document or other file with several people. Answers B and C are incorrect because basic sharing (B) and advanced sharing (C) are preferred because these options are more secure than public file sharing; however, these sharing methods are not as easy to set up. Answer D is incorrect because password sharing is not one of the three methods of sharing.
6. Answer **A** is correct. Network discovery allows this computer to see other network computers and devices and is visible to other network computers. It is enabled or disabled in the Network and Sharing Center. Answer B is incorrect

because the Services console is used to manage your services. Answer C is incorrect because there is no Shared console, although there is a Shared Folder MMC, which is part of the Computer Management console. Answer D is incorrect because there is no Network console. However, there is Network, which allows you to browse network computers and their shared folders and printers.

7. Answer **C** is correct. To access the C: drive remotely, you can use the drive letter\$ administrative share, which is available only to administrators. Therefore, the other answers are incorrect. Answer A is incorrect because C:\Data cannot be accessed remotely. Answers B and D are incorrect because there are no shared folders called C or C.
8. Answer **B** is correct. Windows 7 supports the use of only one Public folder for each computer. Any files that you want to make available publicly can be copied or moved to an appropriate folder inside the Public folder. The Public folder is located at C:\Users\Public. Answer A is incorrect because the Public folder is located at C:\Users\Public, not C:\Public. Answer C is incorrect because the shared folder is not C:\Windows\Public. Answer D is incorrect because the Shared Folder is not C:\Shares\Public.
9. Answer **D** is correct. The ADMIN\$ and IPC\$ are both used by the system during remote administration of the computer. Answer A is incorrect because the NetLogon folder is used by the Net Logon service. Answer B is incorrect because the PRINT\$ share is used during remote administration of printers. Answer C is incorrect because the C\$ is a shared folder to connect to the C drive root directory.
10. Answer **B** is correct. When you use the hosted caching mode, cache resides on a Windows Server 2008 R2 computer that is deployed in the branch office. Answer A is incorrect because Distributed Cache is distributed across client computers in the branch. Answers C and D are incorrect because they are types of cache used in the BranchCache.

*This page intentionally left blank*

## CHAPTER 11

# Managing and Sharing Printers

### **This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Access to Resources:
  - ▶ Configure shared resources
- ▶ Configuring Network Connectivity
  - ▶ Configure networking settings

Users in a home environment mostly print to a local printer directly attached to their home computer. In a business environment, client computers often print to a centralized print server that forwards the print jobs to a print device. Network printing or print sharing allows several people to send documents to a centrally located printer or similar device in an office so that you do not have to connect expensive printers to every single computer in the office. By using a print server, the network administrator can centrally manage all printers and print devices.



# Printer in Windows

- ▶ **Configure shared resources**
- ▶ **Configure networking settings**

## CramSaver

1. In Windows 7, the printer is considered which of the following?
  - A.** The logical device that represents the printer device
  - B.** The physical printer device
  - C.** The network IP address located in DNS
  - D.** The print driver
  
2. What permission do you have to give to a user to change the permissions assigned for a printer?
  - A.** Manage Printers
  - B.** Manage Documents
  - C.** Full Control for Documents
  - D.** Modify permission for Printers
  
3. Where do you find the logs of printer activity as well as printer errors?
  - A.** The System log in the Event Viewer
  - B.** The Application log in the Event Viewer
  - C.** The C:\Windows\Spooler\Logs folder
  - D.** The C:\Windows\System32\Logs folder

## Answers

1. **A** is correct. The printer is the logical representation of the physical printer device. Answer B is incorrect because a physical printer device in Windows is known as the print device. Answer C is incorrect because the only time a printer is assigned to an IP address is when it is a network printer that is connected directly to the network. Answer D is incorrect because the print driver acts as a translator to translate your print jobs to a language that the printer can understand.
2. **A** is correct. To change the permissions, the user has to have the Manage Printers permission. Answer B is incorrect because if a user has the Manage Documents permissions, he or she can only manage documents sent to the print queue. Answers C and D are incorrect because there is neither a Full Control permission nor a Modify permission for printers.

3. **A** is correct. To look at spooler and printer activity, you can use the logs shown in the Event Viewer. The System log shown in the Event Viewer shows printer creation, deletion, and modification. You can also find entries for printer traffic, hard disk space, spooler errors, and other relevant maintenance issues. Answer B is incorrect because the application log shows log events for general applications. Answer C is incorrect because the C:\Windows\Spooler\Logs folder does not exist in Windows 7. Answer D is incorrect because the C:\Windows\System32\Logs folder does not exist in Windows 7. However, there is a C:\Windows\system32\LogFiles folder that holds logs for IIS web server, fax, firewall, MemDiag, WMI, and other items.

The Microsoft definitions of printer-related terms are as follows:

- ▶ **Print device (physical printer):** The physical print device, such as a printer, copy machine, or plotter.
- ▶ **Printer (logical printer):** The printer is the software interface between a print device and the print clients or applications. It is a logical representation of a printer device in Windows that has an assigned printer name and software that controls a printer device. When you print to the printer device, you print to the printer, which then prints to the printer device.
- ▶ **Spooler:** Often referred to as a *queue*, the spooler accepts each document being printed, stores it, and sends it to the printer device when the printer device is ready.
- ▶ **Print driver:** A program designed to enable other programs to work with a particular printer without concerning themselves with the specifics of the printer's hardware and internal language.

### ExamAlert

Make sure you understand the difference between a printer and a print device when taking the exam. A printer is the logical representation and the printer device is the physical representation.

You can connect a print device (printer, plotter, copy machine, or similar device) directly to your Windows 7 computer usually using a Universal Serial Bus (USB) or wireless technology such as Bluetooth or indirectly through a network. You can then print to the printer when running applications on the

Windows 7 computer, or you can share the printer so that other users and network applications can print to the printer over the network.

## Local Versus Network Printing

As an administrator, you can install two types of printers: a local or a network printer. Both types of printers must be created before sharing them for others to use. Table 11.1 lists the advantages and disadvantages of printing to a local printer or a network printer.

**Table 11.1 Comparing Local and Network Printers**

	Local Printer	Network Printer
<b>Advantages</b>	<p>The print device is usually in close proximity to the user's computer.</p> <p>Plug and Play can detect local printers and automatically install drivers.</p>	<p>Many users can access print devices.</p> <p>Network printers support distributing updated printer drivers to multiple clients.</p> <p>The print server manages the printer driver settings.</p> <p>A single print queue appears on every computer connected to the printer, enabling each user to see the status of all pending print jobs, including their own jobs.</p> <p>All users can see the state of the printer.</p> <p>Some processing is passed from the client computer to the print server.</p> <p>You can generate a single log for administrators who want to audit the printer events.</p>
<b>Disadvantages</b>	<p>A print device is needed for every computer.</p> <p>Drivers must be manually installed for every local printer.</p> <p>A local printer takes more processing to print.</p>	<p>The print device might not be physically close to the user.</p> <p>Security is physically limited on the print device.</p>

**Note**

Whether you choose to print locally or on a network, make sure that your system has sufficient memory and free disk space to handle your print jobs.

When you print to a local or network printer, you must have a print driver that is compatible with the print device to which you are printing. The print driver is software used by computer programs to communicate with a specific printer or plotter, which translates the print jobs from a certain platform to information that the printer understands. The print driver also helps define the capabilities of the printer to the system.

As with any driver that you load on a Windows system, it is strongly recommended that you use only device drivers with the Designed for Microsoft Windows 7 or Designed for Microsoft Windows 2008 Server logos. Installing device drivers that are not digitally signed by Microsoft might disable or impair the operation of the computer or allow viruses on to your computer.

**ExamAlert**

Whenever possible, you should use digital signed device drivers. Having a digital signed device driver means that the driver has been tested, verified, and signed by Microsoft so that it is safe for your computer.

**Note**

A computer running Microsoft Windows 7 Professional can also function as a print server. However, it is limited to only 10 network connections.

## Printing Process

When users print a document, most know only to click the print icon or select Print from the File menu and go grab their document from the printer. Of course, a lot happens in the background that gets the document out of the printer.

The following briefly describes the printer process:

1. If a printer is connected directly to its computer, you must load the appropriate driver so that it knows what commands to send to the printer. If a client computer connects to a printer, the print server downloads a print driver to the client computer automatically.

2. When a user prints from an application such as Microsoft Word, he selects the print option or button, and a print job is created. The application calls up the graphical device interface (GDI), which calls the printer driver associated with the target print device. The GDI renders the print job in the printer language of the print device, such as HP's Printer Control Language or Adobe's Postscript, to create an enhanced metafile (EMF). The application then calls the client side of the spooler (Winspool.driv).
3. After it has been formatted, the print job is sent to the local spooler, which provides background printing.
  - ▶ If the print job is being sent to the local print device, it saves it to the local hard drive's spool file. When the printer is available, the print job prints on the local print device.
  - ▶ If the local spooler determines that the job is for a network print device, it sends the job to the print server's spooler. If the local printer is being sent to a shared printer (\\server\printer), the print job goes to the server message block (SMB) redirector on the client. The print server's spooler saves the print job to the print server's hard drive spool file. When the network print device becomes available, the print job prints on the network print device.

The print spooler (spoolsv.exe) manages the printing process, which locates the correct print driver, loads the driver, spools (queues) the print job, and schedules the print job.

## Installing a Printer on Windows 7

If you have the correct permissions to add a local printer or a remote shared printer, use the Add Printer Wizard. After the printer is installed, it then is listed in the Devices and Printers folder.

### Installing Local Printer

To add a local printer to a Windows 7 system, perform the following steps, as illustrated in Figure 11.1:

1. Click the **Start** button and open the **Control Panel**.
2. Under Hardware and Sound, click **View Devices and Printers**.

3. To start the Add Printer Wizard, click **Add a printer**.
4. Select **Add a Local Printer**.

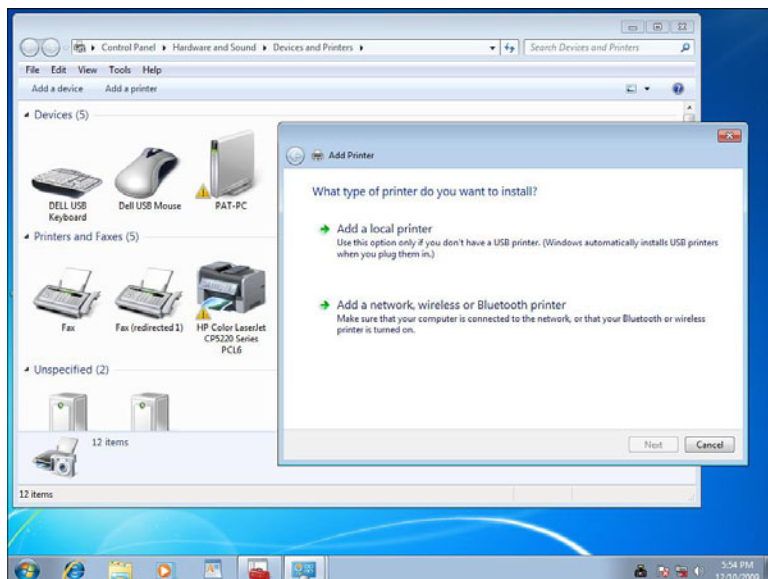


FIGURE 11.1 Choosing between local and network printing.

5. When the Choose a Printer dialog box displays, as shown in Figure 11.2, you specify the port to which the printer is connected. If the port already exists, such as an LPT1 or a network port specified by an IP address, select the port from the **Use an existing port** drop-down list. If the port does not exist, click **Create a new port**, select **Standard TCP/IP Port**, and click **Next** (see Figure 11.3). For the device type, you can select either auto detect, TCP/IP device, or web services device. Then specify the IP address or DNS name of the printer and the Port Name. If you type the address in the hostname or IP address box, it populates the IP address in the port name (see Figure 11.4). It then tries to communicate with the printer using the address you specified.

#### Note

The TCP/IP printer port uses host port 9100 to communicate.

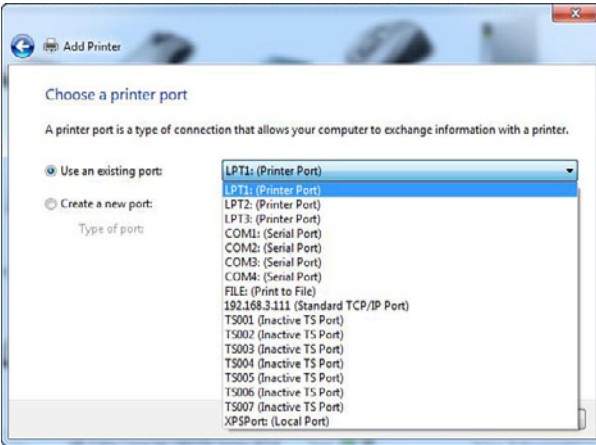


FIGURE 11.2 Choosing a printer port.

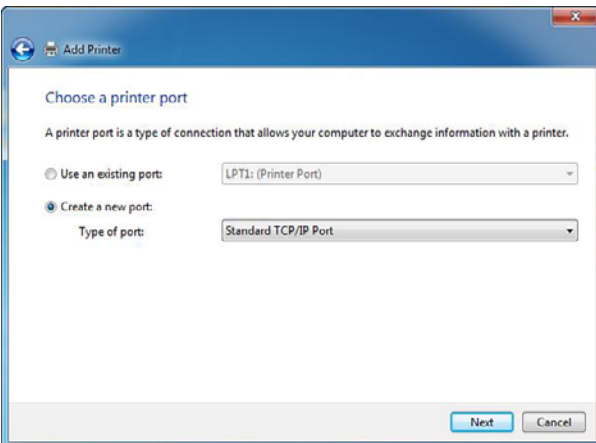


FIGURE 11.3 Creating a new standard TCP/IP device port.

6. If Plug and Play does not detect and install the correct printer automatically, you are asked to specify the printer driver (printer manufacturer and printer model), as shown in Figure 11.5. If the printer is not listed, you have to use the Have Disk option.

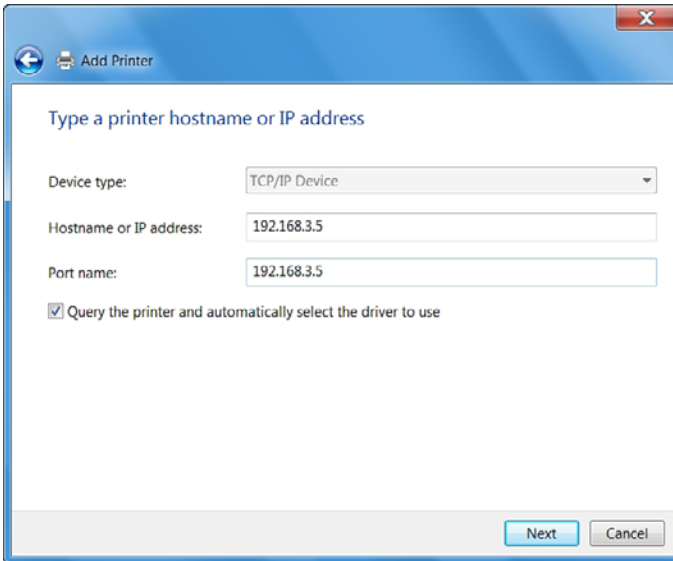


FIGURE 11.4 Specifying the printer hostname or IP address.

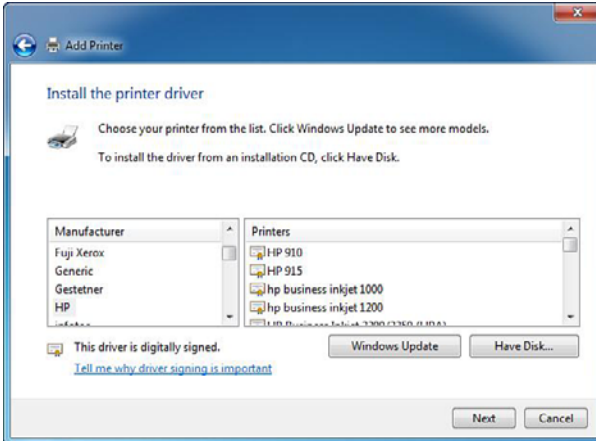


FIGURE 11.5 Installing the printer driver.

7. When the Type a Printer Name dialog box displays, specify the name of the printer. If you want this to be the default printer for the system on which you are installing the printer, select the **Set as the default printer** option. Click the **Next** button.



8. On the Printer Sharing dialog box, specify the share name. You can also specify the Location or Comments. Although Windows 7 supports long printer names and share names including spaces and special characters, it is best to keep names short, simple, and descriptive. The entire qualified name, including the server name (for example, \\Server1\HP4100N-1), should be 32 characters or fewer.
9. When the printer was successfully added, you can print the standard Windows test page by clicking the **Print a test page** button. Click the **Finish** button.

## Install a Network Printer

To add a network printer to a Windows 7 system, perform the following steps:

1. Click the **Start** button and open the **Control Panel**.
2. Under Hardware and Sound, click **View Devices and Printers**.
3. To start the Add Printer Wizard, click **Add a printer**.
4. Select **Add a network, wireless or Bluetooth printer**.
5. If the printer is not automatically found, click **The Printer that I want isn't listed** option to generate the dialog box shown in Figure 11.6.

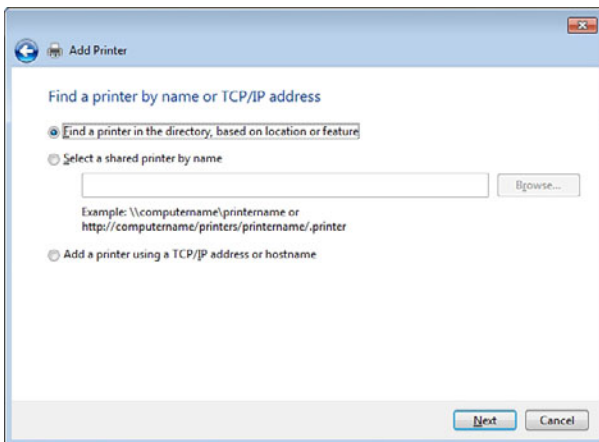


FIGURE 11.6 Specifying the location of a network printer.

6. If you have a printer published in Active Directory (assuming you are part of a domain), you choose **Find a printer in the directory, based on location or feature**. If you know the UNC, you select the **Select a shared printer by name**. If you know the TCP/IP address, choose the last option, **Add a printer using a TCP/IP address or hostname**. Click the **Next** button.
7. In the Type a printer name dialog box, specify the printer name. If you want this to be the default printer for the system you are installing, select **Set as the default printer** option. Click the **Next** button.
8. When the printer is successfully added, you can print the standard Windows test page by clicking the **Print a test page** button. Click the **Finish** button.

## Printer Properties

After installing the logical printer, you can right-click the printer from the Devices and Printers folder and select **Printer Properties** to configure numerous settings. The following tabs enable you to configure the settings:

- ▶ The General tab, as shown in Figure 11.7, enables you to configure the printer name, location, comments, and to print a test page.

If you click the **Preferences** button on the General tab, the default paper size, paper tray, print quality/resolution, pages per sheet, print order (such as front to back or back to front), and number of copies are available. The options that are available vary depending on your printer.
- ▶ The Sharing tab enables you to share a printer. You can also publish the printer in Active Directory if you choose the **List in the directory** option. Because the printer on a server can be used by other clients connected to the network, you can add additional drivers by clicking the **Additional Drivers** button. By default, Windows includes drivers for 32-bit clients (x86 drivers), 64-bit clients (x64), and Itanium PCs.
- ▶ The Ports tab, as shown in Figure 11.8, enables you to specify which port (physical or TCP/IP port) the printer uses as well as to create new TCP/IP ports.
- ▶ The Advanced tab enables you to configure the driver to be used with the printer, the priority of the printer, when the printer is available, and how print jobs are spooled.

- ▶ The Security tab enables you to specify the permissions for the printer.
- ▶ The Device Settings tab enables you to configure the trays, font substitution, and other hardware settings.
- ▶ The Color Management tab ensures that color content is rendered as accurately as possible on both the monitor and the printer.
- ▶ The About tab (not available on all printers) enables you to see the printer and drivers (and their versions) installed for the printer.

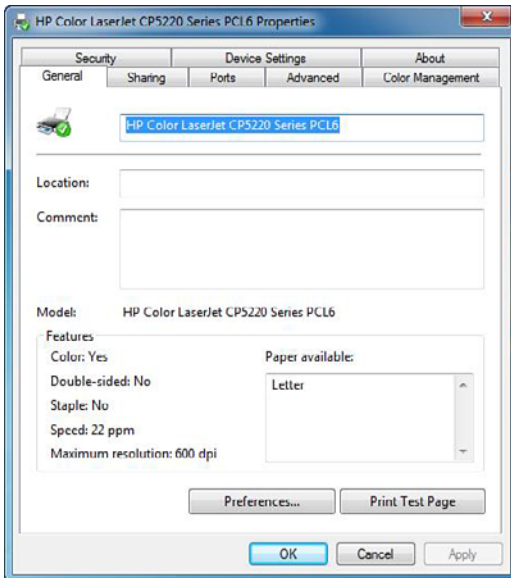


FIGURE 11.7 Printer properties.

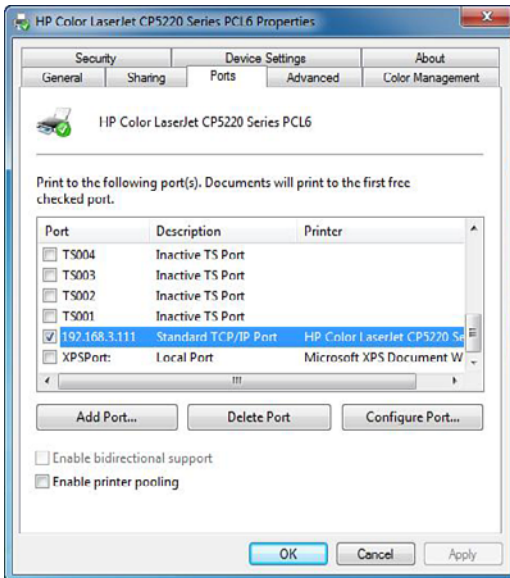


FIGURE 11.8 Configuring the printer ports.

## Location-Aware Printing

If you have a mobile computer that you use in multiple locations, it is likely that you need to print in various locations. With Windows 7 Professional, Ultimate, and Enterprise editions, you define default printers for each network you use. Then instead of manually switching printers when you connect to a network, Windows 7 automatically prints to the local printer:

1. Click the Start menu and select **Devices and Printers**.
2. Select your local printer.
3. Click **Manage Default Printers** in the menu bar.
4. In the Manage Default Printers dialog box, shown in Figure 11.9, click **Change my default printer when I change networks**, specify which printer should be the default for each network, and then click **OK**.
5. From the Select network list, select a network. Then select a printer used in that location. Click the **Add** button.

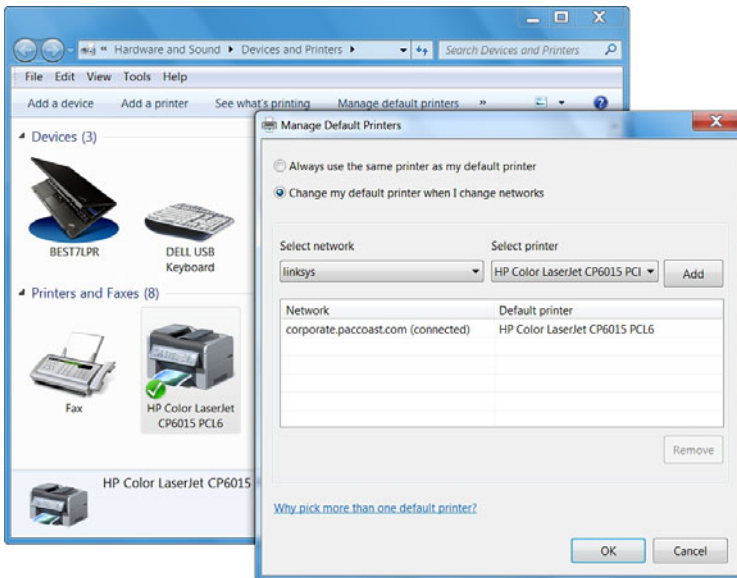


FIGURE 11.9 Configuring location-aware printers.

## Printer Permissions

To control who can use the printer and who can administer the print jobs and printers, use the Security tab to specify printer permissions for those who are not otherwise administrators. Windows provides three basic levels of printer permissions, as shown in Figure 11.10:

- ▶ **Print:** Allows users to send documents to the printer
- ▶ **Manage this printer:** Allows users to modify printer settings and configuration, including the ACL itself
- ▶ **Manage documents:** Provides the ability to cancel, pause, resume, or restart a print job

There is a fourth level of printer permissions called special permissions, which enables you to choose more specific permissions, including

- ▶ Print
- ▶ Manage this printer
- ▶ Manage documents

- ▶ Read permissions
- ▶ Change permissions
- ▶ Take ownership

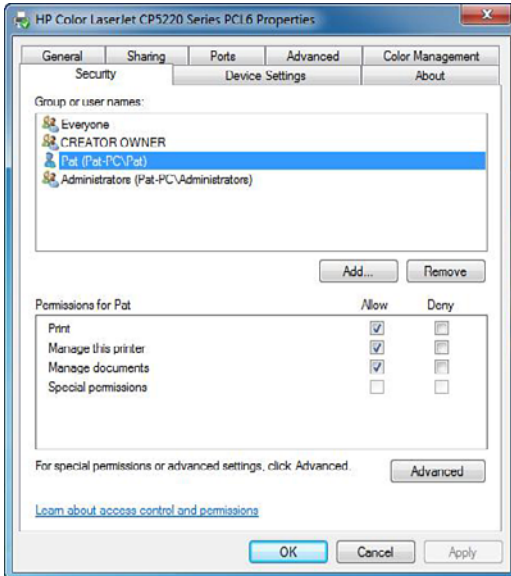


FIGURE 11.10 Printer permissions.

By default, the Print permission is assigned to the Everyone group. If you need to restrict who can print to the printer, you will need to remove the permission and assign the Print permission to other groups or individual users. Much like file permissions, you can deny Print permissions.

The Creator Owner group is granted the allow Manage documents permission. This means that when a user sends a print job to the printer, he can manage his own print job. Administrators, print operators, and server operators have the Manage documents and the Manage the printer permissions.

## Managing the Print Spooler

The print spooler is an executable file that manages the printing process, which includes retrieving the location of the correct print driver, loading the driver, creating the individual print jobs, and scheduling the print jobs for printing.

Typically, the print spooler is loaded during startup and continues to run until the operating system shuts down. You can restart the print spooler by doing the following:

1. Open the **Services** console located in Administrative Tools.
2. Right-click **Print Spooler** and select **Restart**, as shown in Figure 11.11.
3. You can also stop and start the service.

### ExamAlert

If the print spooler becomes unresponsive or you have print jobs that you cannot delete, you should try to restart the Print Spooler service.

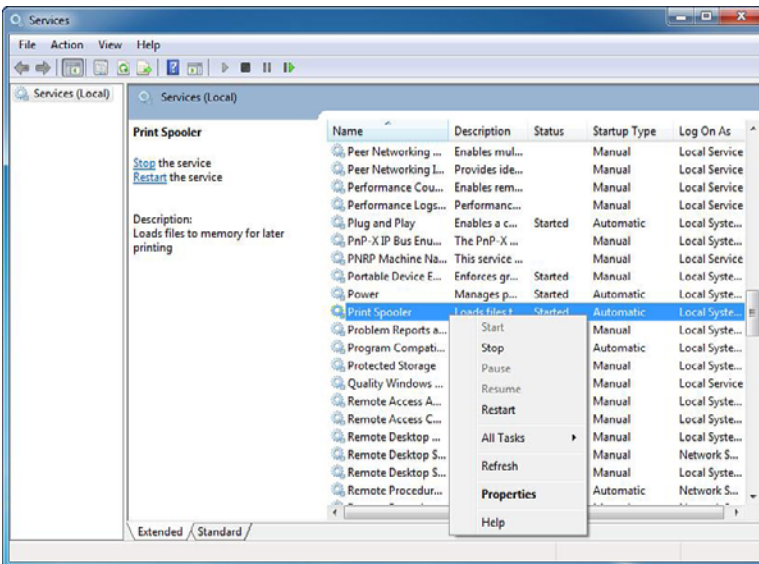


FIGURE 11.11 Print Spooler service in the Services console.

After the print jobs are created, they are stored as files on the hard drive. When the print device is available, the spooler retrieves the next print job and sends it to the print device. By default, the spool folder is located at

%SystemRoot%\System32\Spool\Printers. So, on most installations, this is the C:\Windows\System32\Spool\Printers folder. If the system drive becomes full, the performance of the computer might slow down dramatically, services and applications running on the computer might degrade or not function at all, and the system can become unstable. Because the print spooler is on the same volume that holds the Windows system files, the administrator must ensure that spooling print jobs do not accidentally fill up the system volume.

If your computer running Windows 7 acts as a printer server for multiple users or you are printing multiple large print jobs, you might choose to move the spool folder to another volume if your volume with the Windows folder is close to being full.

#### Note

When you print a Word document or a PDF file, the actual print job sent to the printer is many times larger than the original Word or PDF file itself. Therefore, you should make sure that you have sufficient disk space to hold the print jobs while printing.

## Managing Print Jobs

As a user or an administrator, at times you might need to manage individual print jobs or documents. To view documents waiting to print, do the following:

1. Open the **Devices and Printers** folder.
2. Double-click the printer on which you want to view the print jobs waiting to print.
3. To view the print queue, select **See what's printing**. You can also click **Printer: Ready or # document(s) in queue** at the top of the screen where the # represents how many documents are in the queue, as shown in Figure 11.12.



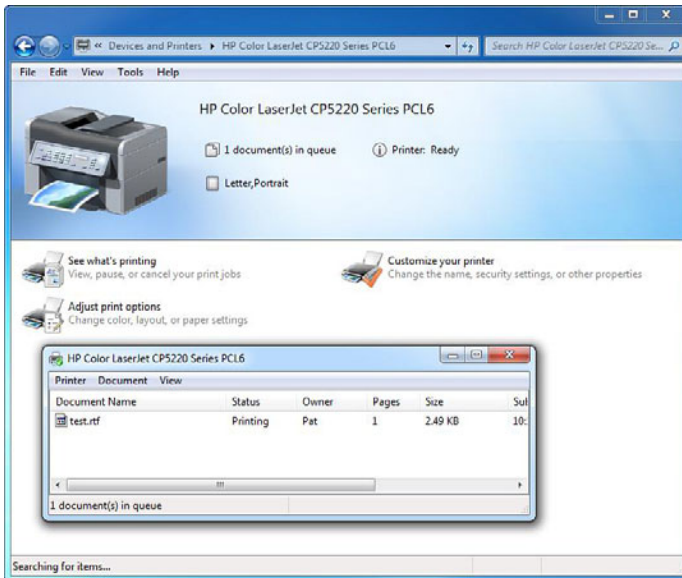


FIGURE 11.12 Viewing documents in the print queue.

The print queue shows information about a document such as print status, owner, and number of pages to be printed. From the print queue, you can cancel or pause the printing of a document that you have sent to the printer. You also can open the print queue for the printer on which you are printing by double-clicking the small printer icon in the Notification area on the taskbar.

To pause a document, open the print queue, right-click the document you want to pause, and select the **Pause** option. If you want to stop printing the document, right-click the document that you want to stop printing and select the **Cancel** option. You can cancel the printing of more than one document by holding down the **Ctrl** key and clicking each document that you want to cancel.

By default, all users can pause, resume, restart, and cancel their own documents. To manage documents that are printed by other users, however, you must have the Manage Documents permission.

## Looking at the Logs

To look at spooler and printer activity, you can use the logs shown in the Event Viewer. By default, the Administrative Events or the System log shows printer creation, deletion, and modification. You can also find entries for

printer traffic, hard disk space, spooler errors, and other relevant maintenance issues. See Figure 11.13.

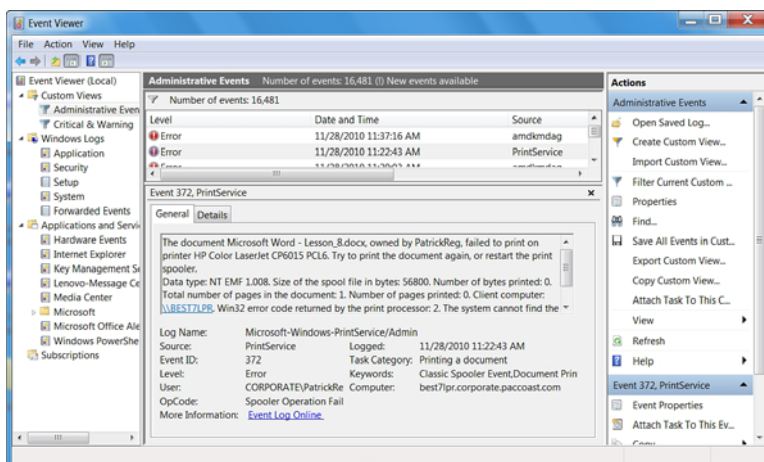


FIGURE 11.13 Administrative Events showing printer activity.

## Auditing Printer Access

Similar to file and folder access, you can also audit printers. You can specify which users or groups and which actions to audit for a particular printer. Before you can do printer auditing, you need to enable an Audit Object Access policy, which is done using local or group policies (Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy). After the policy has taken effect, you would then do the following:

1. Open the **Devices and Printers** folder.
2. Right-click the printer you want to audit and select **Printer Properties**.
3. Choose the **Security** tab.
4. Select the **Advanced** button.
5. Choose the **Auditing** tab.
6. Select **Add** and then choose the groups or users you want to audit.
7. Check the boxes for auditing successful or failed events.
8. Click **OK** to close the Advanced Security Settings box.
9. Click **OK** to close the Printer Properties box.

You would then look in the Security logs in the Event Viewer for inappropriate or unauthorized printing.

## Troubleshooting Printing Problems

When problems occur, you must be ready to troubleshoot those problems. Of course, when looking at what is causing the problem, you need to look at everything that can cause the problems. When it comes to printing, this includes

- ▶ The application attempting to print
- ▶ The logical printer on the local computer
- ▶ The network connection between the local computer and the print server
- ▶ The logical printer on the server
- ▶ The network connection between the print server and the print device
- ▶ The print device itself, including hardware, configuration, and status

The first step is to identify the scope of the failure; in other words, determine what is working and what is failing. For example, if a user can print from one application but not another on the same computer, the problem is most likely related to the application that is having problems printing. If the user can print to other printers with no problem, you should then try to print from another system in an attempt to duplicate the problem. If the problem occurs on multiple computers, you need to focus on the logical printer on the server or the print device. Of course, one place that might give you insight into some problems is the logs in the Event Viewer, specifically if the spooler has written any errors to the event logs.

You can confirm connectivity between the print client and the print server by opening the **Printers and Faxes** folder and double-clicking the printer to open the printer window. If the printer window opens and it shows documents in the print queue, the client is communicating with the print server. If you cannot open the printer window, the problem is with authentication, security permissions, or a network connectivity problem. You can test connectivity further by trying to ping the print server or by clicking the Start button, selecting Search, and typing in \\printservername. Also, make sure that the printer has not been disabled or offline within Windows.

If you suspect that the print server cannot connect to the printer, you should first check to see if the print device is in operation: Make sure that the printer is on and online; make sure that it is connected to the server or network; and make sure that the printer is not showing any errors. Next, from the print server, make sure that the print server can access the print device. You can also make sure that the IP address on the logical printer port matches the address of the print device. You could test network connectivity by pinging the address of the print device.

If you suspect a problem with the print server itself, you need to make sure that the Print service and the remote procedure call (RPC) service is running. You might also try to restart the print service and make sure that you have sufficient disk space on the drive where the spool folder is located.

If you have trouble connecting to a printer on a Windows 7 computer, you can check the Advanced sharing settings and make sure the following settings are on:

- ▶ Network discovery
- ▶ File and printer sharing
- ▶ Sharing in the Public folder sharing section

You can also make sure that the Server service is running on the computer that is hosting the printer and that the workstation service is running on the client. Both of these are on by default for all Windows computers. If pages are only partially printed, check that there is sufficient memory on the printer to print the document. If text is missing, verify whether the missing text uses a font that is valid and installed. Of course, another reason might be that you need to replace the printer's toner cartridge.

If your printed documents have garbled data or strange characters, you should verify that you have the correct print driver loaded for the printer. You might also consider reinstalling the drivers because they could be corrupt. Finally, check for bad cables or electromagnetic interference. See Table 11.2 for a list of common printing problems and how to fix them.

### ExamAlert

Anytime you have garbled data or strange characters, you should always suspect that you have the wrong print driver installed.

TABLE 11.2 Troubleshooting Common Printing Problems

If You Encounter This Problem:	Do This:
Printer server cannot connect to the printer.	<p>Make sure print device is operational (printer is on and online, printer is connected to the server or network, and printer is not showing any errors).</p> <p>Make sure IP address on the logical printer port matches the address of the print device.</p> <p>Try pinging the address of print device.</p>
Print server is having problems.	<p>Make sure that the printer services and remote procedure call (RPC) service is running.</p> <p>Restart the print service.</p> <p>Make sure you have sufficient disk space on the drive where the spool folder is located.</p>
Pages are partially printed.	<p>Check that there is sufficient memory on the printer.</p> <p>Check to see if the printer's toner or ink cartridge needs to be replaced.</p>
Text is missing.	<p>Verify whether the missing text uses a font that is valid and installed.</p> <p>Check to see if the printer's toner or ink cartridge needs to be replaced.</p>
Documents have garbled data or strange characters.	<p>Verify that the correct print driver is loaded on the printer.</p> <p>Reinstall the drivers because they could be corrupt.</p> <p>Check for bad cables.</p> <p>Check for electromagnetic interference.</p>

## Cram Quiz

1. What do you call the component that holds and forwards the print jobs that are sent to the physical printer?
  - A. The print driver
  - B. The spooler
  - C. The PrintTemp folder
  - D. The Processor area

2. What printer permission allows you to modify printer settings and configuration?
- A. Print
  - B. Manage the printer
  - C. Manage documents
  - D. Full Control
3. Which permission is assigned to the Everyone group?
- A. Print
  - B. Manage the printer
  - C. Manage documents
  - D. Full Control

## Cram Quiz Answers

1. **B** is correct. The printer spooler is often referred to as a queue, which accepts each document being printed, stores it, and sends it to the printer device the printer device is ready. Answer A is incorrect because the print driver is a program designed to enable other programs to work with a particular printer without the other programs concerning themselves with the specifics of the printer's hardware and internal language. Answers C and D are incorrect because there is no PrintTemp folder or Processor area in Windows 7.
2. **B** is correct. Manage the printer allows users to modify printer settings and configuration, including the ACL itself. Answer A is incorrect because the Print permission allows users to send documents to the printer. Answer C is incorrect because the Manage documents permission provides the ability to cancel, pause, resume, or restart a print job. Answer D is incorrect because Full Control is not a Printer permission.
3. **A** is correct. The Print permission allows users to send documents to the printer. By default, the Print permission is assigned to Everyone. Answer B is incorrect because the Manage the printer permission allows users to modify printer settings and configuration, including the ACL itself. Answer C is incorrect because the Manage documents provides the ability to cancel, pause, resume, or restart a print job. Answer D is incorrect because Full Control is not a Printer permission.
-

## Review Questions

1. You add a printer directly to the network using a built-in Ethernet card. What port would you use to connect to the printer?
  - A. TCP/IP port
  - B. USB port
  - C. UDP port
  - D. NetBIOS printer
2. What do you call a program designed to enable other programs to work with a particular printer without concerning themselves with the specifics of the printer's hardware and internal language?
  - A. Print device
  - B. Printer
  - C. Spooler
  - D. Print driver
3. You have a shared printer that is installed on a computer running Windows 7. Pat prints a large document several times by mistake. What do you have to do to enable Jane to delete the extra print jobs?
  - A. Configure the printer permissions for Jane to Allow Manage Printers permission
  - B. Configure the printer permission to assign the Allow Manage Documents permission
  - C. Create a new print queue that points to the same print device and assign full permission to Jane
  - D. Configure the Allow Manage queue permission
4. What is the default port if you configure a TCP/IP printer?
  - A. 25
  - B. 80
  - C. 443
  - D. 9100

5. You are the administrator for Acme.com. You have a shared printer called Printer1 connected to a computer running Windows 7 called Win7. You assign the Everyone group the Allow Print permission. When a user tries to print to the \\Win7\Printer1, the user is unable to print. You soon discover that a few other users also cannot print to the same printer. You log on to a computer that has been mapped to the shared printer and try to print several documents to the printer but none will print. You soon discover the following message when you try to access the print queue:

Printer1 on Win7 is unable to connect.

You are able to ping the Win7 computer. What do you need to do to ensure that the print jobs will print? (Choose the best answer.)

- A. On a Windows server, create a share printer that points to \\Win7\Printer1.
  - B. From a command prompt, run `net print \\Win7\printer1`.
  - C. Restart the Print Spooler service on the local computer.
  - D. Restart the Print Spooler service on the print server.
6. What permission do you need for a user to print to a Windows printer?
- A. Print
  - B. Write
  - C. Manage this printer
  - D. Manage documents
7. You have a print job that you cannot delete and it does not finish. What should you try?
- A. Restart the printer
  - B. Restart the server service
  - C. Restart the print spooler
  - D. Make sure the printer is connected
8. Where is the print spooler kept on a computer running Windows 7?
- A. C:\Windows\spool
  - B. C:\Spool
  - C. C:\Windows\System32\Spool\Printers
  - D. C:\Windows\Spool\Printers



9. You enable auditing in Windows 7 so you can keep track of who is using a printer connected to a computer running Windows 7. Where would you find the audit logs so that you can review them?
- A. In the Application logs in the Event Viewer
  - B. In the C:\Logs folder
  - C. In the C:\Windows\System32\Logs folder
  - D. In the Security logs in the Event Viewer
10. You print a document, but all that you get is garbled text. What is the problem?
- A. The print spooler became unresponsive.
  - B. The printer is not using the right ink cartridge.
  - C. The printer has not been calibrated.
  - D. You are using the incorrect driver.

## Review Question Answers

1. Answer **A** is correct. When you have a printer that is connected directly to the network, you can connect to it through a TCP/IP port or through a printer that is shared on a Windows server or a Windows 7 workstation. Answer B is incorrect because a USB port is a local port, not a network port. Answer C is incorrect because UDP is one of the core protocols used in the TCP/IP suite. Answer D is incorrect because NetBIOS provides the mechanism to share files and printers.
2. Answer **D** is correct. A print driver is a program designed to enable other programs to work with a particular printer without concerning themselves with the specifics of the printer's hardware and internal language. In other words, the print driver acts as translator for the printer. Answer A is incorrect because a print device is the physical print device. Answer B is incorrect because a printer is the software interface between a printer device and the print clients or applications. Answer C is incorrect because the spooler accepts each document being printed, stores it, and sends it to the printer device when the printer device is ready.
3. Answer **B** is correct. By default, users can delete their own print jobs. To be able to delete any print job, the user needs to have the Manage documents permission for the printer. Therefore, the other answers are incorrect.
4. Answer **D** is correct. The TCP/IP printer port uses host port 9100 to communicate. Answer A is incorrect because port 25 is used by SMTP. Answer B is incorrect because port 80 is used by HTTP. Answer C is incorrect because port 443 is used by HTTPS.

5. Answer **D** is correct. If the print spooler stalls, you need to stop and restart the service. After deleting the queues, the users need to resubmit their print jobs. Of course, because this affects more than one user, the problem is with Windows 7 computer servicing more than one user and not the local computer. Therefore, Answer C is incorrect. Answer A is incorrect because creating a shared printer on a printer does not overcome the problem that the Win7 computer is having problems communicating with the printer. Answer B is incorrect because running a `net print` command does not fix any printer problems.
6. Answer **A** is correct. The Print permission allows a user to send documents to the printer. Answer B is incorrect because Write is an NTFS permission, not a printer permission. Answer C is incorrect because the Manage this printer permission allows users to modify printer settings and configuration, including the ACL itself. Answer D is incorrect because the Manage documents permission provides the ability to cancel, pause, resume, or restart a print job.
7. Answer **C** is correct. If the print spooler becomes unresponsive or you have print jobs that you cannot delete, you should try to restart the Print Spooler service. Answer A is incorrect because restarting the printer does not clear out the queue because the queue is kept on Windows and sends print jobs when the printer is available. Because you cannot delete print jobs, the printer is not the problem. Answer B is incorrect because the Server service enables your computer to act as a file server. Answer D is incorrect because if the printer is not connected, the print jobs might not be forwarded to the printer. However, the fact that you cannot delete print jobs tells you the problem is with the print queue.
8. Answer **C** is correct. By default, the spool folder is located at `%SystemRoot%\System32\Spool\Printers`. So, on most installations, this is the `C:\Windows\System32\Spool\Printers` folder. If the system drive becomes full, the performance of the server might slow down dramatically, services and applications running on the server might degrade or not function at all, and the system can become unstable. Therefore, the other answers are incorrect.
9. Answer **D** is correct. You look in the Security logs in the Event Viewer for inappropriate or unauthorized printing, assuming auditing is turned on. To enable auditing, you have to use a group policy or a local policy to enable object auditing and then enable auditing on the printer. Therefore, the other answers are incorrect.
10. Answer **D** is correct. If you have the incorrect print driver, you get strange characters, garbled characters, or snippets of programming code. Answer A is incorrect because if the printer spooler becomes unresponsive, the print jobs stay in the print queue and you cannot delete them. Answer B is incorrect because if the printer is not using the right ink cartridge, you might have poor print quality or the colors might be off, but you won't encounter garbled characters. Answer C is incorrect because if the printer is not calibrated, usually something you have to do with some inkjet printers, the colors might be off.

*This page intentionally left blank*

## CHAPTER 12

# Working with Applications

**This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Hardware and Applications:
  - ▶ Configure application compatibility
  - ▶ Configure application restrictions

So far, the preceding chapters have looked at installing and configuring Windows and how to enable some of the common services that Windows can provide; however, you have not yet looked at how to use Windows to run applications. This chapter looks at some of the common applications that come with Windows 7 and how to configure other applications to work with Windows 7.

# Windows Live Essentials

## CramSaver

1. In Windows 7, where do you find the mail program similar to the one that was included with Windows Vista?
  - A. Under Accessories.
  - B. You need to load the Add-on pack included on the Windows 7 installation DVD.
  - C. You need to download and install Windows Live Essentials.
  - D. You need to run Windows Programs and Features and install Windows Mail.

## Answer

1. **C** is correct. Several programs that were in Windows Vista are not included in Windows 7 but are part of Windows Live Essentials, including Windows Live Mail and Windows Live Movie Maker. Therefore, the other answers are incorrect.

Windows 7 includes a wide range of applications so that you can have basic functionality from the start. Some of these applications include WordPad as a basic word processor, Paint as a basic paint program, and Windows Media Player to play videos.

Windows 7 does not have a few productivity applications, such as Windows Mail and photo-editing applications, that were in Windows Vista. If you have a need for these applications, you can access them as part of the Windows Live Essentials suite.

Windows Live Essentials is a suite of freeware applications by Microsoft that aims to offer integrated and bundled email, instant messaging, photo-sharing, blog publishing, security services, and other Windows Live entities. Windows Live Essentials enables users to select and install the following Windows Live software applications:

- ▶ Windows Live Family Safety
- ▶ Windows Live Mail (which includes calendars)
- ▶ Windows Live Messenger

- ▶ Windows Live Movie Maker (Windows Vista and Windows 7 only)
- ▶ Windows Live Photo Gallery
- ▶ Windows Live Sync (integrated with Toolbar and Photo Gallery)
- ▶ Windows Live Toolbar
- ▶ Windows Live Writer
- ▶ Microsoft Office Outlook Connector
- ▶ Microsoft Office Live Add-in
- ▶ Microsoft Silverlight

You can install all the Windows Live Essentials applications except Windows Live Movie Maker on the following operating systems: Windows XP with Service Pack 2 (32-bit edition only), Windows Vista (32-bit or 64-bit editions), Windows 7 (32-bit or 64-bit editions), or Windows Server 2008. Windows Live Movie Maker, unlike the other Essentials programs, is not supported on Windows XP.

To download Windows Live Essentials 2011, visit the following website:  
<http://explore.live.com/windows-live-essentials?os=other>

---

## Cram Quiz

1. Which of the following programs is not included as part of the Windows Live Essentials?
  - A. Windows Live Mail
  - B. Microsoft Outlook
  - C. Windows Live Writer
  - D. Windows Live Messenger

## Cram Quiz Answer

1. Answer **B** is correct. Microsoft Outlook is part of Microsoft Office and not Windows Live Essentials; therefore, the other answers are incorrect.
-

# Application Compatibility

## ► Configure application compatibility

### CramSaver

1. What two methods can you use to run applications that are written for Windows XP that won't normally run under Windows 7?
  - A. Use the application compatibility option
  - B. Run the application as an administrator
  - C. Modify the NTFS permissions of the application
  - D. Use XP Mode
2. What do you call small fixes that may allow applications to run under Windows 7?
  - A. A permission package
  - B. A shim
  - C. A definition
  - D. A language pack

### Answers

1. **A and D** are correct. When an application does not run under Windows 7, you can first try to run the application using the application compatibility option where you specify that Windows should emulate an older operating system. If that does not work, you can also run the application under XP Mode, which allows you to run the program using a virtual computer running Windows XP that runs inside Windows 7. Answers B and C are incorrect because running the application as an administrator or modifying the NTFS permissions of the application do not let the application run in Windows 7.
2. **B** is correct. In Windows 7, Microsoft includes numerous "shims" or minor fixes that are used to improve compatibility with existing non-Microsoft software. Answer A is incorrect because there is no such thing as a permission package. Answer C is incorrect because a definition is an update file used in antivirus software so that it knows of the newest virus. Answer D is incorrect because a language pack is used with certain applications to support languages such as French or Spanish.

Because the Windows 7 architecture is not significantly different from that of Windows Vista, most applications that are written for Windows Vista work in Windows 7. Unfortunately, there are some programs that are written for Windows XP or older versions of Windows that run poorly or not at all. When this occurs, you can change the compatibility settings for the application.

If changing the compatibility settings doesn't fix the problem, go to the program manufacturer's website to see if there is an update for the program.

#### Note

Do not use the Program Compatibility troubleshooter on older antivirus programs, disk utilities, or other system programs because it might cause data loss or create a security risk.

To change compatibility settings using the Program Compatibility Troubleshooter, perform the following steps:

1. Right-click the executable file and select **Troubleshoot Compatibility**.
2. You can first try the recommended settings. If this does not work, select **Troubleshoot program**.
3. When it asks what problems you noticed, select one or more of the following and click the **Next** button:
  - ▶ The program worked in earlier versions of Windows but won't install or run now.
  - ▶ The program opens but doesn't display correctly.
  - ▶ The program requires additional permissions.
  - ▶ I don't see my problem listed.
4. If you selected **The program worked in earlier versions of Windows but won't install or run now**, the wizard asks what version of Windows the program worked on before. Select the appropriate version of Windows and click the **Next** button.
5. If you selected **The program opens but doesn't display correctly**, select one or more of the following options and click the **Next** button:
  - ▶ Error message saying the program needs to run in 256 colors.
  - ▶ Program starts up in a small window (640 × 480 pixel) and won't switch to full screen.



- ▶ Window transparency isn't displayed properly.
  - ▶ Program does not display properly when large scale font settings are selected.
  - ▶ Windows controls appear cut off, or the program changes visual themes when started.
  - ▶ I don't see my problems listed.
6. If you selected **The program requires additional permission**, the wizard tests the application when running with UAC. Click the **Start the program** button. Then click the **Next** button.

To change compatibility settings manually for a program, right-click the program icon, click **Properties**, and then click the **Compatibility** tab, as shown in Figure 12.1. Table 12.1 describes the options available under the Compatibility tab.

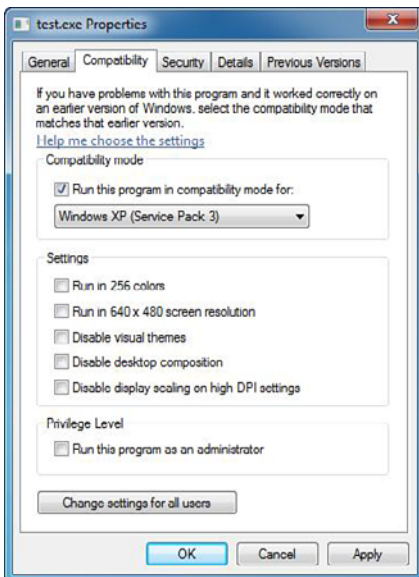


FIGURE 12.1 Application compatibility options.

TABLE 12.1 **Application Compatibility Options**

Option	Description
Compatibility mode	Runs the program using settings from a previous version of Windows. Try this setting if you know the program is designed for (or worked in) a specific previous version of Windows.
Run in 256 colors	Uses a limited set of colors in the program. Some older programs are designed to use fewer colors.
Run in 640 × 480 screen resolution	Runs the program in a smaller-sized window. Try this setting if the graphical user interface appears jagged or is rendered improperly.
Disable visual themes	Disables themes on the program. Try this setting if you notice problems with the menus or buttons on the title bar of the program.
Disable desktop composition	Turns off transparency and other advanced display features. Choose this setting if window movement appears erratic or you notice other display problems.
Disable display scaling on high DPI settings	Turns off automatic resizing of programs if large-scale font size is in use. Try this setting if large-scale fonts are interfering with the appearance of the program. For more information, see Make the text on your screen larger or smaller.
Privilege level	Runs the program as an administrator. Some programs require administrator privileges to run properly. If you are not currently logged on as an administrator, this option is not available.
Change settings for all users	Enables you to choose settings that apply to all users on this computer.

## Microsoft Application Compatibility Toolkit (ACT) and Shims

Besides Windows 7 being a new version of Windows, there are several new technologies that might cause applications to fail. Some of these include the following:

- ▶ **User Account Control (UAC):** Technology that limits administrator level access to a computer running Windows 7.
- ▶ **Windows Resource Protection (WRP):** A mechanism that prevents writing to protected system files or registry locations.
- ▶ **Internet Explorer Protected Mode:** A mechanism used in Internet Explorer that prevents a web page from accessing local computer resources other than the temporary Internet files.

To assist in dealing with compatibility issues, Microsoft created the Application Compatibility Toolkit (ACT), which is a collection of programs that enables administrators to gather information about incompatibilities between specific applications and Windows 7 and deploy fixes to overcome these incompatibilities. Included in ACT, you find the following:

- ▶ Compatibility Administrator
- ▶ Application Compatibility Manager
- ▶ Internet Explorer Compatibility Test Tool
- ▶ Setup Analysis Tool
- ▶ Standard User Analyzer

You can download ACT 5.6 from <http://www.microsoft.com/downloads/en/details.aspx?FamilyId=24DA89E9-B581-47B0-B45E-492DD6DA2971&displaylang=en>. However, to use ACT, you need a SQL server to store the data gathered by ACT. For the SQL server, you can use the full version of SQL or you can use the free versions, SQL Server Express.

Compatibility Administrator is a central database of known compatibility problems for hundreds of Windows 7 applications. In new versions of Windows, Microsoft includes numerous “shims” or minor fixes that are used to improve compatibility with existing non-Microsoft software. Microsoft analyzed the application and provided an application compatibility shim. These shims are applied on a per-application basis. Shims can be used to fool Windows when a specific application is running. For example, if an application checks to see what version of Windows is running, a shim can tell Windows to report a different version of Windows instead of Windows 7. Another example would be that if the application is looking for a file or registry setting that is different between Windows 7 and older versions of Windows, the shim will tell Windows to redirect the application to the correct location.

Of course, although shims are useful tools, they are only temporary bandages for the application until the application can be properly updated to work with the newer version of Windows. In addition, because of revised Windows architecture, shims don’t work for all applications and shims must be created for the application you are trying to get working under Windows 7.

To help ensure application compatibility, the Application Compatibility Manager (ACM) is a tool provided by Microsoft that enables you to analyze and collect information on running applications before you upgrade to or

deploy Windows 7. You can collect information, analyze the data, and test and mitigate your applications.

For more information about ACM, visit the following website:

[http://technet.microsoft.com/en-us/library/cc766464\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc766464(WS.10).aspx)

The Internet Explorer Compatibility Test Tool collects compatibility information for web pages and web-based applications in real-time. When completed, it can identify compatibility problems with web applications and pages for Internet Explorer 8.

The Setup Analysis Tool is designed to analyze application setup programs for potential issues, including the installation of kernel mode drivers, installation of 16-bit components, installation of graphical identification, and authentication (GINA) DLLs and changes to system files and registry keys that are protected with the Windows Resource Protection (WRP).

UAC limits what an application can do, even if logged in as administrator. As a result, the Standard User Analyzer analyzes an application while it's running to determine if an application is compatible with UAC and give you a set of recommended compatibility fixes. After you review the fixes, you can click **Apply** to test the fixes to see if they worked.

## XP Mode

Although most applications written for Windows XP also run on Windows 7, there are still quite a few applications that do not. If a shim is not available, you can use Windows XP Mode to run older applications on your Windows 7 desktop. Windows XP Mode was primarily designed to help businesses move from Windows XP to Windows 7. It isn't optimized for graphic-intensive programs such as 3D games, nor is it suited for programs with hardware requirements such as TV tuners.

Windows XP Mode enables you to run a virtual Windows XP machine in its own window. Much like a physical machine running Windows XP, you can still access the computer resources including drives and other hardware devices. In addition, when you install an application in Windows XP Mode, it appears within the Windows XP window and the Windows 7 application list.

To run Windows XP Mode, you need to be running Windows 7 Professional, Enterprise, or Ultimate edition. You are also recommended to have 2 GB of memory and an additional 15 GB of hard disk space per virtual Windows environment.

When Windows 7 was introduced, Windows XP Mode required a computer that is capable of hardware virtualization (Intel-VT or AMD-V virtualization) and a BIOS that supports hardware virtualization. Virtualization must also be enabled in the BIOS Setup program. Since then, the Windows XP Mode components have been upgraded to allow Windows XP Mode to run without these requirements.

To use Windows XP Mode, you should first download and install Windows Virtual PC, which is the program that runs virtual operating systems on your computer. Then, you can download and install Windows XP Mode, which is a fully licensed version of Windows XP with Service Pack 3.

To download and install Windows Virtual PC, do the following:

1. Go to the Windows XP Mode and Windows Virtual PC website.
2. In the Windows 7 system type drop-down list, click **32-bit** or **64-bit** depending on what version of Windows 7 you're currently running. In the Windows XP Mode language drop-down list, click the language you want to use for Windows XP Mode and then click **Download Windows Virtual PC**. To find out whether you have a 32-bit or 64-bit version of Windows 7, click the **Start** button, right-click **Computer**, and then click **Properties**. The information appears under System, next to System type.
3. Click **Open** to install the program immediately, or click **Save** to save the installation file to your computer and then double-click the file.
4. Click **Yes** to install Update for Windows (KB958559).
5. If you accept the license terms, click **I Accept**.
6. After installation is complete, click **Restart Now** to restart your computer.

After your computer restarts, you should see Windows Virtual PC and Windows XP Mode listed in your list of programs. If you haven't installed Windows XP Mode yet, you can click it to install the program.

To download and install Windows XP Mode:

1. Click the **Start** button, click **All Programs**, click **Windows Virtual PC**, and then click **Windows XP Mode**.
2. In the Windows XP Mode dialog box, click **Download** to go back to the Windows XP Mode and Windows Virtual PC webpage.

3. In the Windows 7 system type drop-down list, click **32-bit** or **64-bit** depending on what version of Windows 7 you're currently running. In the Windows XP Mode language drop-down list, click the language you want to use and then click **Download Windows XP Mode**.
4. Click **Open** to install the program immediately; or click **Save** to save the installation file to your computer and then double-click the file. For best practice, you should click **Save** and keep the file on your computer in case you ever need to reinstall Windows XP Mode.
5. In the Welcome to Setup for Windows XP Mode dialog box, click **Next**.
6. Choose the location for the virtual hard disk file that Windows XP Mode uses or accept the default location and then click **Next**.
7. On the Setup Completed screen, select the **Launch Windows XP Mode** checkbox and then click **Finish**.
8. If you accept the license terms, click **I accept the license terms**, and then click **Next**.
9. On the Installation folder and credentials page, accept the default location where Windows XP Mode files are stored or enter a new location.
10. Enter a password, enter it again to confirm it, and then click **Next**.
11. On the Help protect your computer screen, choose whether you want to protect your computer by turning on automatic updates and then click **Start Setup**.

After setup is complete, Windows XP Mode opens in a separate window.

When you install a program in Windows XP Mode, the program becomes available for use in both Windows XP Mode and Windows 7.

To install and use a program in Windows XP Mode, follow these steps:

1. In Windows 7, click the **Start** button, click **All Programs**, click **Windows Virtual PC**, and then click **Windows XP Mode**.
2. In Windows XP Mode, insert the program's installation disc into your computer's CD/DVD drive; or browse to the program's installation file, open the file, and follow the instructions to install the program.
3. Click the **Close** button at the top of the Windows XP Mode window.
4. In Windows 7, click the **Start** button, click **Windows Virtual PC**, click **Windows XP Mode Applications**, and then click the program you want to open.

For more information about XP Mode, visit the following website:

<http://windows.microsoft.com/en-US/windows7/install-and-use-windows-xp-mode-in-windows-7>

---

## Cram Quiz

1. You have a customized accounting application that was written for Windows XP. Unfortunately, it does not run under Windows 7. What should you do?
  - A. Run the application under XP Mode
  - B. Modify the privilege level for the application to run as a standard user
  - C. Run the MST transform on the application
  - D. Run the application under 256 colors
2. What do you call a package of multiple shims bundled together by Microsoft?
  - A. A MSI package
  - B. XP package
  - C. Microsoft Application Compatibility Toolkit
  - D. Microsoft Application Reconfig Kit

## Cram Quiz Answers

1. **A** is correct. You need to run the application under Windows XP Mode because the enhanced security in Windows 7 does not allow the application to run. Modifying the privilege level or running the program under 256 colors does not allow the program to run under Windows 7. Therefore, Answers B and D are incorrect. Answer C is incorrect because MST transforms are used to install executables that are not available as an MSI file using group policies.
  2. **C** is correct. In new versions of Windows, Microsoft includes numerous “shims” or minor fixes that are used to improve compatibility with existing non-Microsoft software. Microsoft analyzed the application and provided an application compatibility shim. These shims are bundled together with the Microsoft ACT are applied on a per-application basis. They are not bundled in an MSI package or an XP package. Therefore, Answers A and B are incorrect. Answer D is incorrect because there is no such thing as a Microsoft Application Reconfig Kit.
-

# Software Restrictions

► **Configure application restrictions**

## CramSaver

1. What are the two tools used to restrict what applications a user can run on Windows 7? (Select all that apply.)
  - A.** AppLocker in group policies
  - B.** System Configuration tool
  - C.** Software restriction policy in group policies
  - D.** Application Compatibility Toolkit
2. Which of the following is NOT a rule you can create with software restrictions?
  - A.** Hash
  - B.** Path
  - C.** Certificate
  - D.** Location

## Answers

1. **A** and **C** are correct. You can use group policies to restrict which software, specifically software restriction policies and AppLocker. Answer B is incorrect because the System Configuration tool is a valuable tool used to troubleshoot boot problems, particular with programs that start during boot or services. Answer D is incorrect because the Application Compatibility Toolkit is used to load band aids or shims for non-Microsoft applications to function under Windows 7.
2. **D** is correct. The four types of rules used with software restrictions include hash, certificate, path, and zone. Location is not a method for software restrictions. Answers A, B, and C are incorrect because they are valid rules that you can create with software restrictions.

They can be assigned to a site, domain, or organizational unit in Active Directory. Many of these settings can also be set locally on a workstation, which are known as local policies.



To increase security, you can also use local policies and group policies to restrict which software can run a computer. Software restriction policies can be used to:

- ▶ Fight viruses and other forms of malware
- ▶ Regulate which ActiveX controls can be downloaded
- ▶ Run only digitally signed scripts
- ▶ Ensure that only approved software is installed on system computers
- ▶ Lock down the computer

To restrict software, you must first create a software restriction policy that consists of security levels, rules, and settings. A policy consists of a default rule about whether programs are allowed to run (unrestricted) and exceptions to that rule (disallowed). The default rule can be set to Unrestricted or Disallowed. When you use the unrestricted rule as the default, you then specify which programs are not allowed to run as exceptions. When you use the restricted rule as the default, you then specify which programs are allowed to run as exceptions.

To identify which software can run or not run, you create rules based on the following criteria (in order of precedence):

- ▶ **Hash:** A cryptographic fingerprint based on a mathematical calculation of the file that uniquely identifies a file regardless where it is accessed or what it is named, as shown in Figure 12.2
- ▶ **Certificate:** A software publisher certificate used to digitally sign a file
- ▶ **Path:** The local or universal naming convention (UNC) path and name of where the file is stored
- ▶ **Zone:** Internet Explorer security zone

You can also use group policies to install software; specifically, you can install Windows Installer packages (.MSI files), Transform Files (.MST files), and patch files (.MSP files).

### ExamAlert

If you suspect a conflict rules, remember that the order of precedence is hash rules, certificate rules, path rules, zone rules, and default rules.

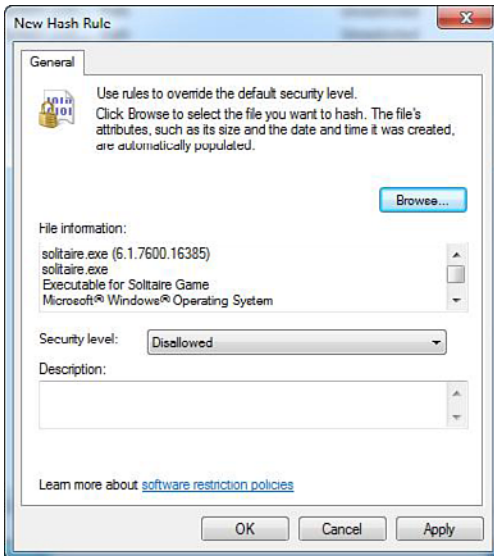


FIGURE 12.2 Software restrictions.

A new feature added to Windows 7 Ultimate and Enterprise is AppLocker, which enables IT professionals to specify exactly what is allowed to run on user desktops. It enables users to run the applications, installation programs, and scripts they need to be productive while still providing the security, operational, and compliance benefits of application standardization.

If AppLocker and the software restriction policy are configured for the same Group Policy Object (GPO), only the AppLocker settings are enforced on computers running Windows 7. Because earlier versions of Windows do not support AppLocker, they still receive the software restriction settings and not the AppLocker settings. Although AppLocker is an additional Group Policy mechanism, it includes the following new enhancements:

- ▶ The ability to define rules based on attributes derived from a file's digital signature, including the publisher, product name, file name, and file version.
- ▶ A more intuitive enforcement model—only a file that is specified in an AppLocker rule is allowed to run.
- ▶ A user interface accessed through an extension to the Local Policy snap-in and Group Policy Management snap-in.

- ▶ An audit-only enforcement mode that enables administrators to determine which files are prevented from running if the policy were in effect.
- ▶ Besides setting policies for .exe files, you can also set policies for .msi files, scripts, and DLLs.

Creating rules based on the digital signature of an application helps make it possible to build rules that don't need to be updated when a new version of the application is released. When testing AppLocker, carefully consider how you will organize rules between linked Group Policy Objects (GPOs). If a GPO does not contain the default rules, either add the rules directly to the GPO or add them to a GPO that links to it. Figure 12.3 shows the Getting Started window for using AppLocker.

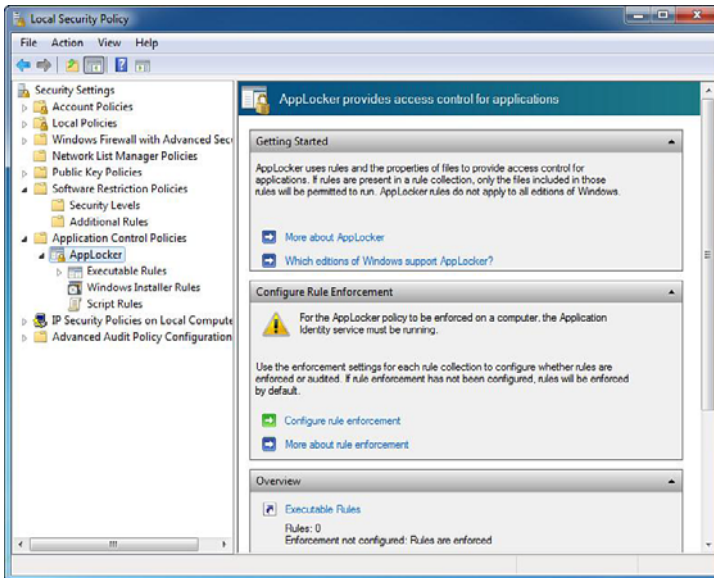


FIGURE 12.3 AppLocker.

Specifically, the default rules enable the following:

- ▶ All users to run files in the default Program Files directory
- ▶ All users to run all files signed by the Windows operating system
- ▶ Members of the built-in Administrators group to run all files

By creating these three rules, you automatically prevent all non-administrator users from being able to run programs that are installed in their user profile directories. You can re-create these rules at any time.

If you want to lock down a user computer, which protects the user and your network, you can use AppLocker to use signatures so that you can identify genuine applications. However, you need to ensure that all of the files that you want your users to run are digitally signed. Unfortunately, this is beyond the scope of the book. If any applications are not signed, consider implementing an internal signing process to sign unsigned applications with an internal signing key.

To allow only signed applications to run, do the following:

1. Open the Local Security Policy MMC snap-in by typing `secpol.msc` in the Search programs and files box.
2. Double-click **Application Control Policies** and then double-click **AppLocker** in the console tree.
3. Right-click **Executable Rules** and then click **Create New Rule**.
4. When the Before You Begin page appears, click **Next**.
5. When the Permissions page appears (see Figure 12.4), click **Next** to accept the default settings.

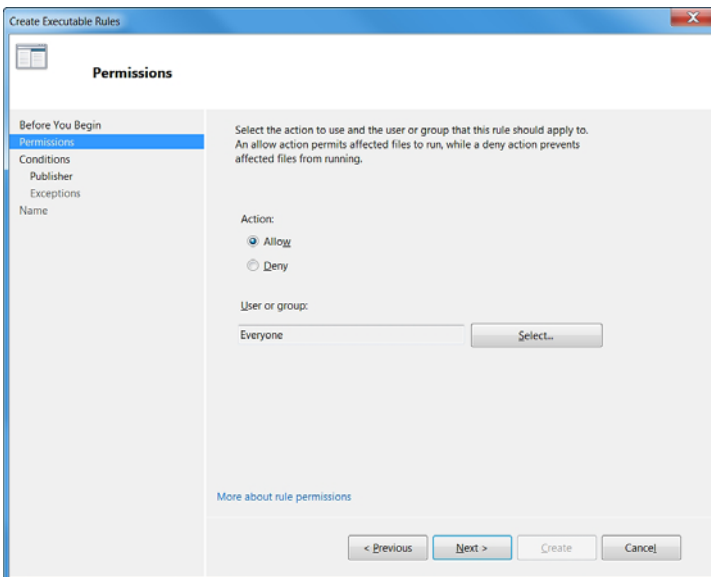


FIGURE 12.4 Configuring permissions for AppLocker rules.

- When the Conditions page appears (see Figure 12.5), click **Next**.

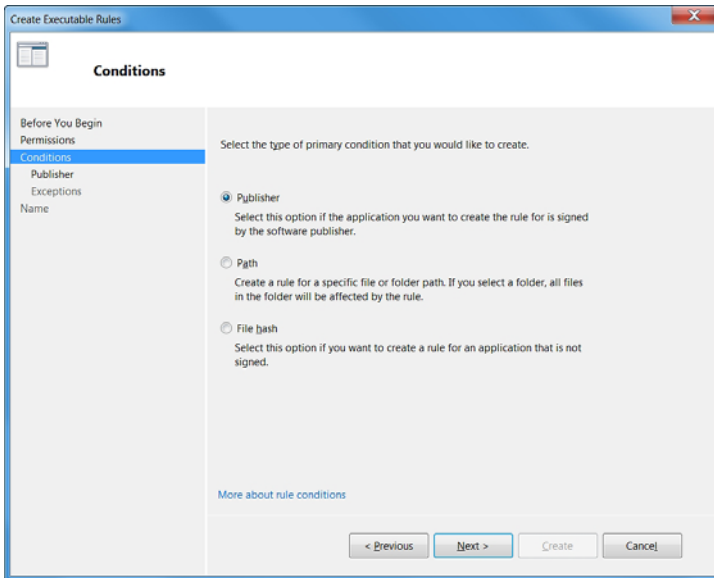


FIGURE 12.5 Configuring conditions for AppLocker rules.

- When the Publisher page appears, select any executable file using the Browse button. Then move the slider to the top to Any publisher, as shown in Figure 12.6. Then click **Next**.
- When the Exceptions page appears, click **Next**.
- When the Name and Description page appears, you can accept the default name or type a custom name and description. Then click **Create**.

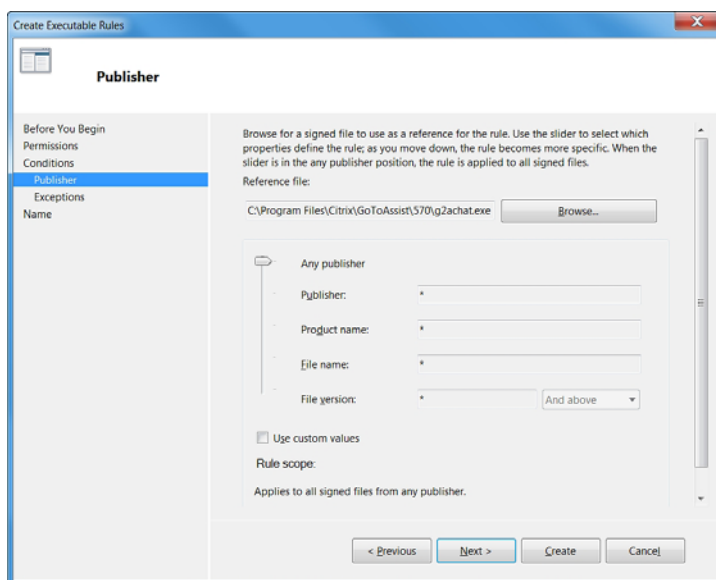


FIGURE 12.6 Configuring AppLocker Publisher rules.

For this work, you must also define a default rule that prevents standard users from running Per-user Applications. The default rule is created by doing the following:

1. Open the Local Security Policy MMC snap-in by entering `secpol.msc` in the Search programs and files box.
2. Double-click Application Control Policies and then double-click **AppLocker** in the console tree.
3. Right-click **Executable Rules** and in the resulting drop-down menu shown in Figure 12.7, click **Create Default Rules**.

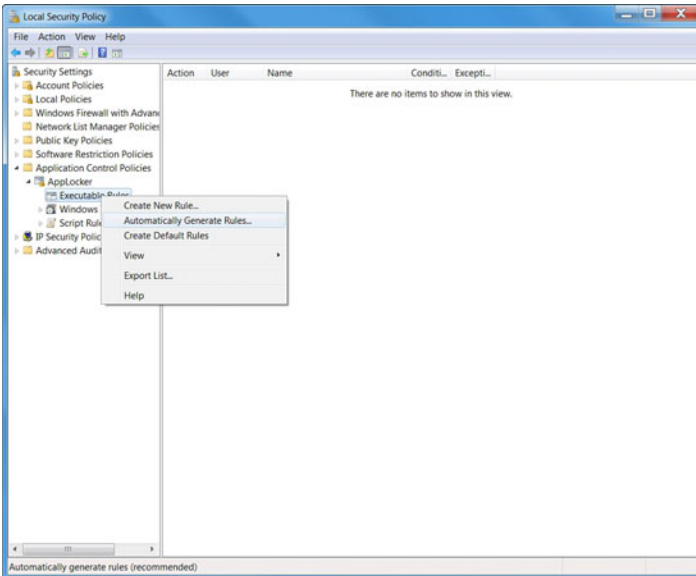


FIGURE 12.7 Create default rules in AppLocker.

---

## Cram Quiz

1. You are trying to use a software restriction policy to block a new game called GV.EXE. So, you make a policy based on the path. However, you soon find out that some users just renamed the GV.EXE to a different name to get around the policy. What can you do to overcome this?
  - A. Use a certificate rule
  - B. Use a Hash rule
  - C. Use a Path rule
  - D. Use a Zone rule
2. When using AppLocker, what are your rules based on?
  - A. File passwords
  - B. NTFS permissions of file
  - C. Size of the file
  - D. File's digital signature

## Cram Quiz Answers

- 1. B** is correct. If you use a Hash rule, you can block the software regardless of where the file is accessed or what it is named. Answer A is incorrect because a certificate uses a digital certificate assigned to a file. Answer C is incorrect because the path did not work in the past and setting a new path can only be circumvented again. Answer D is incorrect because the zone is based on the Internet Explorer security zone.
  - 2. D** is correct. Creating rules based on the digital signature of an application helps make it possible to build rules that don't need to be updated when a new version of the application is released. Therefore, the other answers are incorrect.
-



# Review Questions

1. Which application can be used to test compatibility issues with UAC?
  - A. Compatibility Administrator
  - B. Application Compatibility Manager
  - C. Setup Analyzer Tool
  - D. Standard User Analyzer
2. Which application is used to test web applications and web pages for compatibility problems with Internet Explorer 8?
  - A. Compatibility Administrator
  - B. Application Compatibility Manager
  - C. Internet Explorer Compatibility Test Tool
  - D. Standard User Analyzer
3. How do you enable and configure AppLocker?
  - A. The Registry
  - B. Group Policies
  - C. Control Panel
  - D. Computer Management console
4. Which of the following will AppLocker not support?
  - A. .exe file
  - B. .dll file
  - C. .msi file
  - D. Office document files
5. You upgraded your computer running Windows XP with SP2 to Windows 7 Professional. When you run the widget.exe program, you receive the following error message:

This application is only designed to run on Windows XP or later.

What should you do?
  - A. You should run the application with elevated privileges.
  - B. You should run the application in VGA mode.
  - C. You should install Windows XP Mode and run the application under Windows XP mode.
  - D. You should make sure your machine has all of the Windows updates.

6. You are having problems running a non-Microsoft application. Where can you get help in overcoming this problem? (Choose three answers.)
- A. Check to see if the software vendor has an update
  - B. Look in the Microsoft Application Compatibility Toolkit
  - C. Load the application in XP Mode
  - D. Recompile the program
7. For you to run Windows XP Mode, which of the following are not requirements? (Choose two answers.)
- A. 2 GB of memory
  - B. A video card with 512 MB of memory
  - C. Processor and motherboard that supports hardware virtualization
  - D. 15 GB of additional free disk space.
8. Which editions of Windows 7 can Windows XP Mode be used on? (Choose all that apply.)
- A. Windows 7 Professional
  - B. Windows 7 Enterprise
  - C. Windows 7 Home Premium
  - D. Windows 7 Ultimate
9. Which type of rule would you use when creating a software restriction policy that blocks an application based on an exact location and name of the executable file?
- A. Hash
  - B. Certificate
  - C. Path
  - D. Zone
10. Where do you configure an individual application to run as an administrator?
- A. Under a local security policy
  - B. Use System Configuration Tool
  - C. Computer Management Tool
  - D. Application Compatibility Options under the application properties

## Review Question Answers

1. Answer **D** is correct. UAC limits what an application can run, even if logged in as administrator. As a result, the Standard User Analyzer analyzes an application to identify compatibility problems with Windows 7 User Account Control. Answer A is incorrect because the Compatibility Administrator is a central database of known compatibility problems for hundreds of Windows 7 applications. Answer B is incorrect because the Application Compatibility Manager (ACM) is a tool provided by Microsoft that enables you to analyze and collect information on running applications before you upgrade to or deploy Windows 7. Answer C is incorrect because the Setup Analyzer Tool is designed to analyze application setup programs for potential issues, including the installation of kernel mode drivers, installation of 16-bit components, installation of graphical identification, and authentication (GINA) DLLs and changes to system files and registry keys that are protected with the Windows Resource Protection (WRP).
2. Answer **C** is correct. The Internet Explorer Compatibility Test Tool collects compatibility information for web pages and web-based applications in real-time. When completed, it can identify compatibility problems with web applications and pages for Internet Explorer 8. Answer A is incorrect because the Compatibility Administrator is a central database of known compatibility problems for hundreds of Windows 7 applications. Answer B is incorrect because the Application Compatibility Manager (ACM) is a tool provided by Microsoft that enables you to analyze and collect information on running applications before you upgrade to or deploy Windows 7. Answer D is incorrect because the Standard User Analyzer analyzes an application to identify compatibility problems with Windows 7 User Account Control.
3. Answer **B** is correct. Software Restrictions and AppLocker are used to allow or disallow applications from running on a Windows 7 computer. Both software restrictions and AppLocker are configured through Group Policies including the computer's local policy. Answer A is incorrect because the Registry is a centralized database that contains configuration information for Windows, applications, and hardware devices. Answer C is incorrect because although the Control Panel is the primary configuration tool for Windows 7, the Control Panel is not used to configure software restrictions. Answer D is incorrect because the Computer Management console is used to perform most administrative tasks for Windows.
4. Answer **D** is correct. AppLocker is used to allow or disallow .exe files, .msi files, scripts, and DLLs. AppLocker does not allow or disallow data files, including office document files. Therefore, the other answers are incorrect.
5. Answer **C** is correct. When an application does not run under Windows 7 that was written for an older version of Windows, you should try compatibility mode or run the application under Windows XP Mode. Because the application needs to run under Windows XP Mode, running under elevated privileges or in VGA mode does not work. Therefore, Answers A and B are incorrect. Answer D is incorrect because Windows updates do not allow the application to run under Windows 7.

6. Answers **A**, **B**, and **C** are correct. You should always look to see if the vendor has an update. You can also look in the Microsoft Application Compatibility Toolkit. If that does not work, you can always try to load the application in XP Mode. Answer D is incorrect as you typically cannot recompile the program because you do not typically have the source code and recompiling the program requires special skills and software.
7. Answers **B** and **C** are correct. To run Windows XP mode, you need a minimum of 2 GB of memory (Answer A) and an additional 15 GB of free disk space (Answer D). When Windows 7 was first released, you needed a computer that was capable of hardware virtualization (Intel-VT or AMD-V virtualization) and a BIOS that supports hardware virtualization (Answer C). You do not need additional memory on the video card (Answer B) to run Windows XP Mode.
8. Answers **A**, **B**, and **D** are correct. To run Windows XP Mode, you need to be running Windows 7 Professional, Enterprise, or Ultimate edition. Answer C is incorrect because Windows 7 Home Premium does not run in Windows XP Mode.
9. Answer **C** is correct. The path criteria specify the local or universal naming convention (UNC) path and name of where the file is stored. Answer A is incorrect because the hash criteria is based on a cryptographic fingerprint based on a mathematical calculation of the file that uniquely identifies a file regardless of where it is accessed or what it is named. Answer B is incorrect because the certificate criteria are based on a software publisher certificate used to digitally sign a file. Answer D is incorrect because the zone criteria is based on the Internet Explorer security zone.
10. Answer **D** is correct. If you right-click the executable and select properties, you can select the Compatibility tab to configure what OS to run under, 256 colors, 640 × 480 resolution, and privilege level. Answer A is incorrect because local policies can only be used to restrict an application, not to elevate an application when it runs. Answer B is incorrect because the System Configuration Tool is used to troubleshoot startup problems. Answer C is incorrect because although it includes many tools within a single console, none of them are used for configuring individual applications.

*This page intentionally left blank*

## CHAPTER 13

# Working with Internet Explorer 8.0

### **This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Hardware and Applications:
  - ▶ Configure application compatibility
  - ▶ Configure Internet Explorer

A web browser is the client program or software that you run on your local machine to gain access to a web server. It receives commands, interprets the commands, and displays the results. It is strictly a user-interface/document presentation tool. It knows nothing about the application to which it is attached and only knows how to take the information from the server and present it to the user. It also able to capture data entry made into a form and gets the information back to the server for processing. Because these browsers are used to search and access webpages on the Internet and can be used by an organization's website or provide interface to a program, you need to understand how to configure, customize, and troubleshoot browser issues.

Microsoft Internet Explorer (IE) is the most common browser available because it comes with every version of Windows. Windows 7 includes Internet Explorer 8.0, which has new functionality while reducing online risks.

# Features of Internet Explorer 8.0

- ▶ **Configure application compatibility**
- ▶ **Configure Internet Explorer**

## CramSaver

1. You have a user who is accessing a website located on your company's local intranet. When the user accesses the website, he is prompted for a username and password. How can you make the authentication occur automatically?
  - A. Change the authentication for the website to anonymous
  - B. Add the website's URL to the Local Intranet zone
  - C. Add the website's URL to Trusted Sites zone
  - D. Change the credentials in the Credential Manager
  
2. What can you use to prevent Internet Explorer from saving any data while browsing the Internet?
  - A. Use BranchCache
  - B. Use InPrivate Browsing
  - C. Turn on the use of cookies
  - D. Disable the save data option in the Internet zone
  
3. What can you use to easily invoke an online service by using only the mouse?
  - A. Cookies
  - B. ActiveX
  - C. Accelerators
  - D. SmartScreen Filter

## Answers

1. **B** is correct. When you add the website to the Local Intranet zone, Internet Explorer automatically tries to use your Windows username and password. Answer A is incorrect because if you choose anonymous for the website, the website is not secure. Answer C is incorrect because adding a website to the Trusted Sites zone does not automatically use your Windows username and password. Answer D is incorrect because using Credential Manager does not automatically use your Windows username and password.

2. **B** is correct. InPrivate Browsing (new to IE 8) enables you to surf the Web without leaving a trail in Internet Explorer. This helps prevent anyone else who might be using your computer from seeing what sites you visited and what you looked at on the Web. Answer A is incorrect because BranchCache is used to cache data at a local site so that it does not always have to download the data over a slower WAN link. Answer C is incorrect because cookies are necessary for some sites, and they usually store information so that a website can automatically identify you and your settings on a particular website. Answer D is incorrect because there is no disable the save data option in the zones.
3. **C** is correct. An accelerator is a form of selection-based search that enables a user to invoke an online service from any other page using only the mouse. Answer A is incorrect because a cookie is a message given to a web browser by a web server, which is typically stored in a text file on the PC's hard drive to identify users for websites and possibly prepare customized webpages for them. Answer B is incorrect because ActiveX is a set of controls used to make a webpage more functional. Answer D is incorrect because a SmartScreen Filter includes protection from socially engineered malware that helps identify sites that have been labeled as an imposter or harmful (in other words, phishing).

Compared to Internet Explorer 6 and older version, the most obvious difference in Internet Explorer 8.0 is its redesigned streamlined interface, which is simpler and less cluttered. As a result, IE 8.0 maximizes the space available for display of webpages. In addition to a simpler interface, Internet Explorer 8.0 introduced tabs that enable you to open multiple webpages in a single browser window. If you have a lot of tabs, you can use Quick Tabs to easily switch between open tabs.

Other features in Internet Explorer 8.0 include the following:

- ▶ The Instant Search box lets you search the Web from the Address bar. You can also search using different search providers to get better results.
- ▶ Internet Explorer lets you delete your temporary files, cookies, webpage history, saved passwords, and form information from one place. Delete selected categories or everything at once.
- ▶ Click the Favorites Center button to open the Favorites Center to manage favorites, feeds, and history in one place.
- ▶ Printing now scales webpages to fit the paper you're using. Print Preview gives more control when printing, with manual scaling and an accurate view of what you're about to print.



- ▶ By subscribing to a feed, you can get updated content, such as breaking news or your favorite blog, without having to visit the website.
- ▶ The Zoom feature lets you enlarge or reduce text, images, and some controls.
- ▶ Suggested sites suggest websites when you do not input a valid website address.
- ▶ A new security mode, called InPrivate, helps protect privacy by preventing one's browsing history, temporary Internet files, from data, cookies, usernames, and passwords from being retained by the browser.
- ▶ Accelerators are a form of selection-based search that allows a user to invoke an online service from any other page using only the mouse.
- ▶ Web slices are snippets of an entire page to which a user can subscribe. Web slices are kept updated by the browser automatically and can be viewed directly from the Favorites bar.
- ▶ SmartScreen Filter includes protection from socially engineered malware, which helps identify sites that have been labeled as an imposter or harmful (in other words, phishing).
- ▶ Full-page zoom now reflows the text to remove the appearance of horizontal scrollbars on zooming.
- ▶ If a website or add-on causes a tab to crash in Internet Explorer 8, only that tab is affected, leaving the other tabs unaffected.

For more information about Internet Explorer, visit the following website:

<http://www.microsoft.com/windows/products/winfamily/ie/default.mspx>

## Internet Explorer Zoom

Internet Explorer Zoom lets you enlarge or reduce the view of a webpage. Unlike changing font size, zoom enlarges or reduces everything on the page, including text and images. You can zoom from 10% to 1000%.

To zoom a webpage, do the following:

1. On the bottom right of the Internet Explorer screen, click the arrow to the right of the Change Zoom Level button.

2. Do one of the following:

- ▶ To go to a predefined zoom level, click the percentage of enlargement or reduction you want.
- ▶ To specify a custom level, click **Custom**. In the Percentage zoom box, type a zoom value and then click **OK**.

If you have a mouse with a wheel, hold down the Ctrl key and then scroll the wheel to zoom in or out. If you click the Change Zoom Level button, it cycles through 100%, 125%, and 150%, giving you a quick enlargement of the webpage. From the keyboard, you can increase or decrease the zoom value in 10% increments. To zoom in, press Ctrl + plus sign. To zoom out, press Ctrl + minus sign. To restore the zoom to 100%, press Ctrl + 0.

## Common Internet Explorer Settings

Most of the configuration options for Internet Explorer are accessed by starting Internet Explorer, clicking the **Tools** button and selecting **Internet Options**. You can also access them from the Internet Options applet in the Control Panel. The Internet Options dialog box has several tabs, including General, Security, Privacy, Content, Connections, Programs, and Advanced, as shown in Figure 13.1.

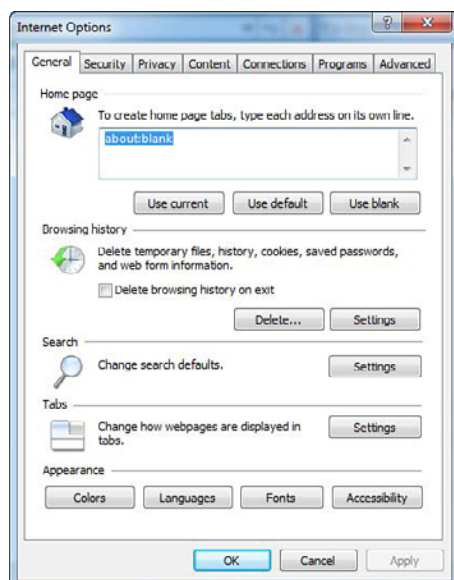


FIGURE 13.1 Internet Explorer Options dialog box.

At the top of the General tab, you can configure the home page or the default page that is loaded when you start Internet Explorer. This enables you to have your favorite search engine, news, website, portal, or an organization's internal website load automatically when you start Internet Explorer. By going to a webpage and then clicking the **Use Current** button, you make the page that is currently being displayed your home page. You can also configure it to show a blank page. Of course, to make the change take effect, you have to click the **Apply** or **OK** button.

Some organizations might configure the organization's home page as the default home page so that users cannot make changes to Internet Explorer using group policies. Other times, if you are experiencing an unexpected change in the home page, it was most likely caused by visiting a particular website (usually you have to click on **Yes** to change the website, but that is not always the case), installing a program that changes the Internet Explorer home page, or being infected by a virus or spyware.

Below the home page, you find the section to configure browsing history including how Internet Explorer uses temporary Internet files, which is used as a disk cache for Internet browsing. When you visit a website, parts of the webpage (such as pictures, sound, and video files) are copied on the system as a temporary Internet file so that on future visits to that site, it loads faster. If you click on the **Settings** button, you can configure the browser to check for newer versions of the saved page on every visit, every time you start Internet Explorer, automatically, or never. If you need to force Internet Explorer to reload a fresh webpage, you can hold down the Shift key while you click **Refresh**, or press **Shift+F5**. You can also click the **View Files** button to view the temporary Internet files.

You can determine how much disk space you want to use as a cache and where the folder is located that stores the temporary files. If you click on **View Files**, you open the folder that stores the temporary files so that you can inspect them directly.

History specifies the number of days that Internet Explorer should keep track of your viewed pages in the History list. IE creates shortcuts to pages you viewed in this and previous browsing sessions. If you are low on disk space, you might want to decrease the number. You can also clear your history from here.

The AutoComplete feature remembers previous entries that you made for web addresses, forms, and passwords. When you type information in one of these fields, AutoComplete suggests possible matches. These matches can include folder and program names you type into the Address bar, as well as search queries, stock quotes, or other information that you type in forms on webpages.

To use AutoComplete, start typing the information in the Address bar, in a field on a webpage, or in a box for a user name or password. If you have typed a similar entry before, AutoComplete lists possible matches as you type. If a suggestion in the list matches what you want to enter in that field, click the suggestion. If no suggestion matches what you are typing, continue typing.

To select AutoComplete settings in Internet Explorer, click **Tools** and then click **Internet Options**. On the Content tab, click **Settings** in the AutoComplete section. You can specify whether you want to use AutoComplete for web addresses, forms, user names, and passwords. You can also clear the history of previous AutoComplete entries. When typing information in web forms, and when typing passwords, you can remove an item from the list of suggestions by clicking the item and then pressing the Delete key.

As shown in Figure 13.2, if you click the **Advanced** tab, you can configure a wide range of configuration options, including disabling script debugging, enabling folder view for FTP sites, enabling a personalized favorites menu, enabling notification when downloads are complete, enabling automatic image resizing, and playing sounds and videos in webpages. It also has several security features, such as emptying temporary Internet Files when the browser is closed, enabling Profile Assisting, using SSL 2.0 or 3.0 (needed to connect to secure webpages as indicated by https://), warning about invalid site certificates, and warning if a form is being redirected.

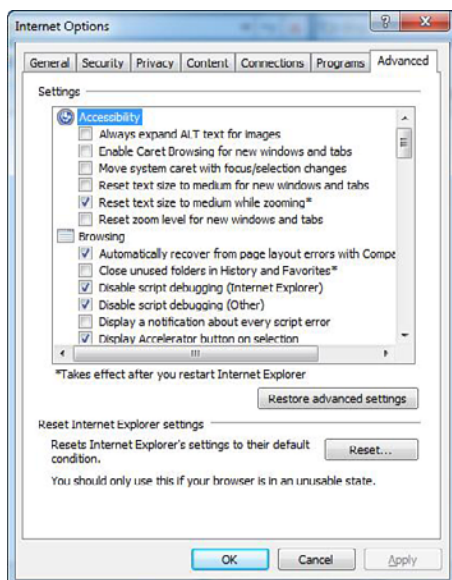


FIGURE 13.2 Advanced settings in Internet Explorer.

## Plug-Ins/Add-Ons and Scripting Languages

To make Internet Explorer more powerful and more flexible and by adding additional functionality, Internet Explorer has the capability to use add-ons and scripting languages. The four basic add-ons supported by IE are

- ▶ Toolbars and extensions
- ▶ Search providers
- ▶ Accelerators
- ▶ InPrivate filtering

An add-in (also known as plug-in) is a software module that adds a specific feature or service to the browser to display or play different types of audio or video messages. Common plug-ins are Shockwave, RealMedia (RealAudio and Real Video), and Adobe Reader (used to read Portal Document Format (PDF)).

In an effort to make browsing more functional, web developers created and enable active content. Active content, which is based on various add-ins, is done by using small executable or script code that is executed and shown within the client's web browser. Unfortunately, this feature is an added security risk where some scripts could be used to perform harmful actions on a client machine. Some of the most popular types of active content are VBScript, JavaScript, and ActiveX components.

To view current Add-ons, click the **Tools** button, click **Manage Add-ons**, and then click **Enable or Disable Add-ons**. In the Show box, select one of the following options:

- ▶ To display a complete list of the add-ons that reside on your computer, click **All Add-ons**.
- ▶ To display only those add-ons that were needed for the current webpage or a recently viewed webpage, click **Currently loaded Add-ons**.
- ▶ To display add-ons that were pre-approved by Microsoft, your computer manufacturer, or a service provider, click **Add-ons that run without permission**.
- ▶ To display only 32-bit ActiveX controls, click **Downloaded Controls**.

When you run an add-on for the first time, Internet Explorer asks permission, which should notify you if a website is secretly trying to run malicious code.

Internet Explorer has a list of pre-approved add-ons that have been checked and digitally signed. The add-on list can come from Microsoft, your computer manufacturer, your Internet Service provider (if you are using a private branded version of Internet Explorer), or your corporation's network administrator. The add-ons in this list are run without displaying the permissions dialog.

Add-ons are typically fine to use, but sometimes they force Internet Explorer to shut down unexpectedly. This can happen if the add-on was created for an earlier version of Internet Explorer or has a programming error. When you encounter a problematic add-on, you can disable it and/or report it to Microsoft. If disabling add-ons doesn't solve the problem, try resetting Internet Explorer to its default settings.

To permanently disable an add-on, do the following:

1. Click the **Tools** button and then click **Manage Add-ons**.
2. In the Show list, click **All add-ons**.
3. Click the add-on you want to disable (as shown in Figure 13.3) and then click **Disable**.
4. When you are finished, click the **Close** button.

To re-enable an add-on, you click the **Enable** button.

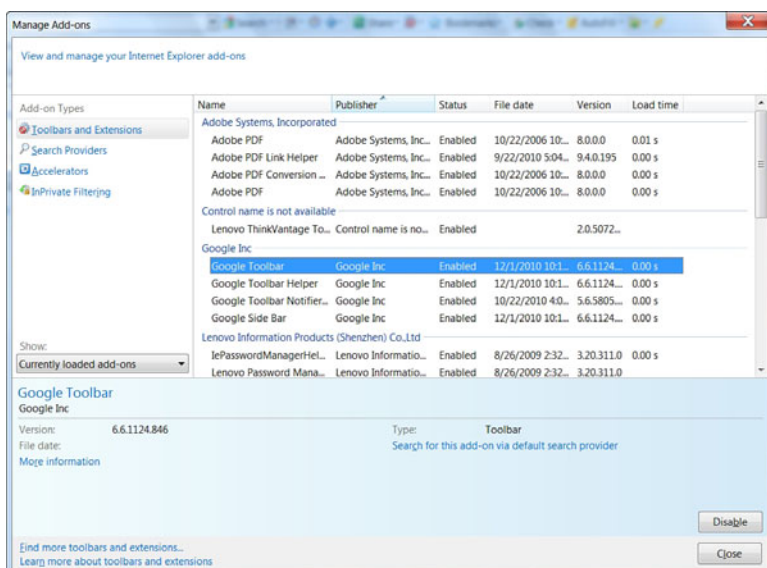


FIGURE 13.3 Managing add-ons.

To temporarily disable all add-ons, follow these steps:

1. Click the **Start** button and click **All Programs**.
2. Click **Accessories**.
3. Click **System Tools**.
4. Click **Internet Explorer (No Add-ons)**.

You can only delete ActiveX controls that you have downloaded and installed. You cannot delete ActiveX controls that were pre-installed or add-ons of any kind, but you can disable them. To delete an ActiveX control that you have installed, use Programs and Features in Windows Control Panel.

## Internet Explorer Security Features

Internet Explorer offers a number of features to help protect your security and privacy when you browse the Web. They include

- ▶ **Phishing Filter:** Helps protect you from online phishing attacks, fraud, and spoofed websites
- ▶ **Protected Mode:** Helps protect you from websites that try to save files or install programs on your computer
- ▶ **Pop-up Blocker:** Helps block most pop-up windows
- ▶ **Add-on Manager:** Enables you to disable or allow web browser add-ons and delete unwanted ActiveX controls
- ▶ **Notification:** Notifies you when a website is trying to download files or software to your computer
- ▶ **Digital signatures:** Tells you who published a file and whether it has been altered since it was digitally signed
- ▶ **128-bit secure (SSL) connection for using secure websites:** Helps Internet Explorer create an encrypted connection with websites such as banks and online stores

## Cookies and Privacy Settings

As spyware has become more common, the need to protect your personal information, including browser history, has grown. A cookie is a message given to a web browser by a web server, which is typically stored in a text file

on the PC's hard drive. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized webpages for them. When you enter a website using cookies, you might be asked to fill out a form providing some information, such as your name and interests. This information is packaged into a cookie and sent to your web browser, which stores it for later use. The next time you go the same website, your browser sends the cookie to the web server. The server can use this information to present you with custom webpages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it. Some uses of cookies include keeping track of what a person buys, using online ordering systems, personalizing a website, storing a person's profile, storing user IDs, and providing support to older web browsers that do not support host header names. A cookie cannot be used to get data from your hard drive, get your email addresses, or steal sensitive information about you.

From the General tab, you can delete the cookies that are stored on your hard drive. By clicking the Privacy tab, you can adjust the tab slider on the privacy scale to determine how much of your personal information can be accessed by websites and whether a website can save cookies on your computer.

To view privacy settings, select the Privacy tab from the Internet Options dialog box. To adjust your privacy settings, adjust the tab slider to a new position on the privacy scale. A description of the privacy settings that you select displays on the right side of the tab slider. The default level is Medium; it is recommended that you configure Medium or higher. You can also override the default for cookies in each security zone. In addition, you can override certain settings (automatic cookie handling and session cookies) by clicking the **Advanced** button, or you can allow or block cookies from individual websites by clicking the **Edit** button.

Many websites provide privacy statements that you view. A site's privacy policy tells you what kind of information the site collects and stores and what it does with the information. Information that you should be mostly concerned with is how the websites use personally identifiable information such as your name, email addresses, address, and telephone number. Websites also might provide a Platform for Privacy Preferences (P3P) privacy policy, which can be used by browsers to filter cookie transactions on the basis of a cookie's content and purpose. To view the Privacy Report, open the View menu and click **Privacy Report**. To view a site's privacy statement, select the website and click on the **Summary** button.



## Content Zones

Typically when you are surfing the Internet, there are certain sites that you visit often and there are other sites which you visit for the first time. Typically, you tend to trust those sites that you visit often and you are less trusting of new sites, especially sites that are not popular. To help manage Internet Explorer security when visiting sites, Internet Explorer divides the network connection into four content types, which are as follows:

- ▶ **Internet Zone:** Anything that is not assigned to any other zone and anything that is not on your computer, or your organization's network (intranet). The default security level of the Internet zone is Medium.
- ▶ **Local Intranet Zone:** Computers that are part of the organization's network (intranet) that do not require a proxy server, as defined by the system administrator. These include sites specified on the Connections tab, network paths such as \\computername\foldername, and local intranet sites such as http://internal. You can add sites to this zone. The default security level for the Local internet zone is Medium=Low, which means Internet Explorer allows all cookies from websites in this zone to be saved on your computer and be read by the website that created them. Lastly, if the website requires NTLM or integrated authentication, it automatically uses your username and password.
- ▶ **Trusted Sites Zone:** Contains trusted sites that from which you believe you can download or run files without damaging your computer or data or that you consider are not security risks. You can assign sites to this zone. The default security level for the Trusted sites zone is Low, which means Internet Explorer allows all cookies from websites in this zone to be saved on your computer and be read by the website that created them.
- ▶ **Restricted Sites Zone:** Contains sites that you do not trust from which downloading or running files might damage your computer or data or that are considered a security risk. You can assign sites to this zone. The default security level for the Restricted sites zone is High, which means Internet Explorer blocks all cookies from websites in this zone.

For each of the web content zones, there is a default security level. The security levels available in Internet Explorer are

- ▶ **High:** Excludes any content that can damage your computer.
- ▶ **Medium:** Warns you before running potentially damaging content.
- ▶ **Low:** Does not warn you before running potentially damaging content.

- ▶ **Custom:** A security setting of your own design. Use this level to customize the behavior of Active Data Objects (AD) and Remote Data Services (RDS) objects in a specific zone.

Whenever you access a website, Internet Explorer checks the security settings for the zone of the website. To tell which zones the current webpage falls into, you look at the right side of the Internet Explorer status bar. Besides adjusting the zones or assigning the zones or assigning a website to a zone, you can also customize settings for a zone by importing a privacy settings file from a certificate authority.

To modify the security level for a web content zone, do the following:

1. Click the **Tools** button and then click **Internet Options**.
2. In the Internet Options dialog box, on the Security tab, click the zone on which you want to set the security level.
3. Drag the slider to set the security level to **High**, **Medium**, or **Low**. Internet Explorer describes each option to help you decide which level to choose, as shown in Figure 13.4. You are prompted to confirm any reduction in security level. You can also choose the **Custom level** button for more detailed control.
4. Click **OK** to close the Internet Options dialog box.

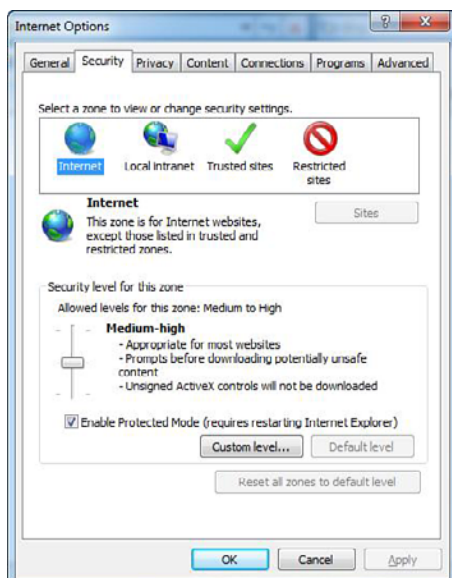


FIGURE 13.4 Security options within Internet Explorer.

Software publisher certificates (third-party digital certificates) are used to validate software code such as Java or ActiveX controls or plug-ins. Depending on the security settings for a zone, when software code is accessed from a website you automatically download the software code, disable the software code, or prompt to download the software code via a security warning. If you open the Tools menu and select **Internet Options**, select the **Security** tab, and click the **Custom Level** button, you can select **enable**, **disable**, or **prompt** to download ActiveX controls (signed and unsigned) and scripting of Java applets.

To view the certificates for Internet Explorer, open the Internet Options dialog box, click the **Content** tab and click on the **Certificates** button. To see list of certificates, click the appropriate certificates. From here, you can also import and export individual certificates.

## Dynamic Security and Protected Mode

Because threats can come from any place at any time, Internet Explorer has added several features to protect your system. Dynamic Security options for Internet Explorer 8.0 offer multiple security features to defend your computer against malware and data theft. The Security Status Bar keeps you notified of the website security and privacy settings by using color-coded notifications next to the address bar. Some of these features include

- ▶ Address Bar turns green to indicate website bearing new High Assurance certificates, indicating the site owner has completed extensive identity verification checks.
- ▶ Phishing Filter notifications, certificate names, and the gold padlock icon are now also adjacent to the address bar for better visibility.
- ▶ Certificate and privacy detail information can easily be displayed with a single click on the Security Status Bar.
- ▶ The Address Bar is displayed to the user for every window, whether it's a pop-up or standard window, which helps to block malicious sites from emulating trusted sites.
- ▶ To help protect you against phishing sites, Internet Explorer warns you when visiting potential or known fraudulent sites and blocks the site if appropriate. The opt-in filter is updated several times per hour with the latest security information from Microsoft and several industry partners.
- ▶ International Domain Name Anti-Spoofing notifies you when visually similar characters in the URL are not expressed in the same language.

To protect your system even further, Internet Explorer includes the following features:

- ▶ ActiveX Opt-in disables nearly all pre-installed ActiveX controls to prevent potentially vulnerable controls from being exposed to attack. You can easily enable or disable ActiveX controls as needed through the Information Bar and the Add-on Manager.
- ▶ Cross-Domain Barriers limits scripts on webpages from interacting with content from other domains or windows. This enhanced safeguard helps to protect against malicious software by limiting the potential for malicious websites to manipulate flaws in other websites or cause you to download undesired content or software.

If Internet Explorer is still using its original settings, you see the Information bar in the following circumstances:

- ▶ If a website tries to install an ActiveX control on your computer or run an ActiveX control in an unsafe manner.
- ▶ If a website tries to open a pop-up window.
- ▶ If a website tries to download a file to your computer.
- ▶ If a website tries to run active content on your computer.
- ▶ If your security settings are below recommended levels.
- ▶ If you access an intranet webpage, but have not turned on intranet address checking.
- ▶ If you started Internet Explorer with add-ons disabled.
- ▶ If you need to install an updated ActiveX control or add-on program.
- ▶ The webpage address can be displayed with native language letters or symbols, but you don't have the language installed.

When you see a message in the Information bar, click the message to see more information or to take action.

To stop the information bar from blocking file and software downloads, do the following:

1. Click to open **Internet Explorer**.
2. Click the **Tools** button and then click **Internet Options**.
3. Click the **Security** tab and then click **Custom level**.

4. Do one or both of the following:

- ▶ To turn off the Information bar for file downloads, scroll to the Downloads section of the list and then, under Automatic prompting for file downloads, click **Enable**.
- ▶ To turn off the Information bar for ActiveX controls, scroll to the ActiveX controls and plug-ins section of the list and then, under Automatic prompting for ActiveX controls, click **Enable**.

5. Click **OK**, click **Yes** to confirm that you want to make the change, and then click **OK** again.

Table 13.1 lists some of the more common messages that might appear in the Information bar, along with a description of what each message means.

TABLE 13.1 **Common Messages Found in Internet Explorer 8.0**

Message	What It Means
To help protect your security, Internet Explorer stopped this site from installing an ActiveX control on your computer. Click here for options.	The webpage tried to install an Active X control and Internet Explorer blocked it. If you want to install the ActiveX control and you trust the publisher of the ActiveX control, right-click the information and select Install Software.
Pop-up blocked. To see this pop-up or additional options, click here.	Pop-up Blocker has blocked a pop-up window. You can turn Pop-up Blocker off or allow pop-ups temporarily by clicking the Information bar.
This website is using a scripted window to ask you for information. If you trust this website, click here to allow scripted windows.	Internet Explorer has blocked a website that tried to display a separate window such as a login screen in an attempt to gather confidential information. If you trust the website, click the Information bar and click select Temporarily Allow Scripted Windows or Allow websites to prompt for information using scripted windows customer security setting.
To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options.	A webpage tried to download a file that you might not have requested. If you want to download the file, click the Information bar and then click Download File.
Your security settings do not allow websites to use ActiveX controls installed on your computer. This page may not display correctly. Click here for options.	The website tried to install an ActiveX control but your security settings did not allow it. This is caused when a website is listed in the Restricted Site list. If you trust the site, remove the site from the Restricted site. If the problem still exists, try adding the site to the Trusted sites list.

TABLE 13.1 **Continued**

Message	What It Means
Internet Explorer has blocked this site from using an ActiveX control in an unsafe manner. As a result, this page may not display correctly.	A website tried to access an ActiveX control on your computer without your permission.

Internet Explorer's protected mode is a feature that makes it more difficult for malicious software to be installed on your computer. In addition, it enables users to install wanted software when they are logged in as a standard user instead of an administrator. Protected mode is turned on by default and an icon appears on the status bar to let you know that it's running. When you try to install software, protected mode warns you when webpages try to install software or if a software program runs outside of protected mode. If you trust the program and want to allow it to run on any website, select the **Always allow websites to use this program to open web content** checkbox.

### ExamAlert

Protected mode makes it more difficult for malicious software to be installed on your machine.

If you suspect problems caused by Protected Mode, you can try the following:

- ▶ Move the site to the Trusted Sites zone
- ▶ Disable protected mode in IE
- ▶ Modify the application

## InPrivate Browsing

InPrivate Browsing (new to IE 8) enables you to surf the Web without leaving a trail in Internet Explorer. This helps prevent anyone else who might be using your computer from seeing what sites you visited and what you looked at on the Web. You can start InPrivate Browsing from the New Tab page, as shown in Figure 13.5, or the Safety button.

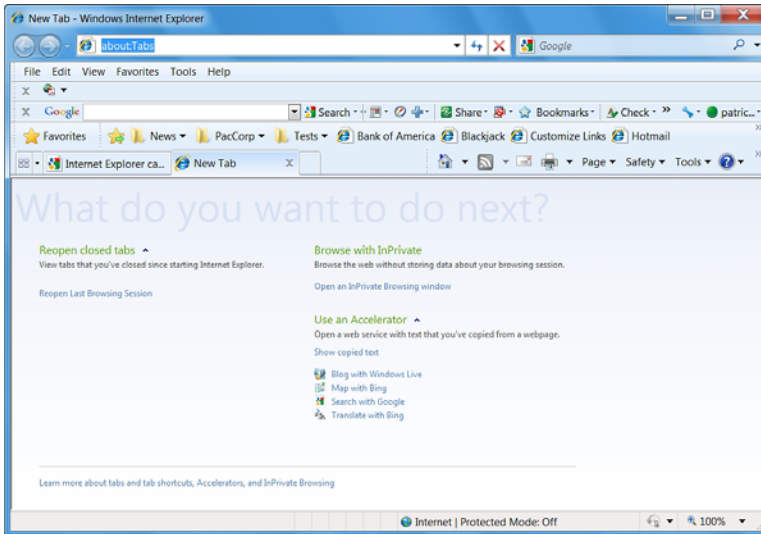


FIGURE 13.5 The New Tab page.

When you start InPrivate Browsing, Internet Explorer opens a new browser window. The protection that InPrivate Browsing provides is in effect only during the time that you use that window. You can open as many tabs as you want in that window, and they are all protected by InPrivate Browsing. However, if you open another browser window, that window is not protected by InPrivate Browsing. To end your InPrivate Browsing session, close the browser window.

While you are surfing the Web using InPrivate Browsing, Internet Explorer stores some information (such as cookies and temporary Internet files) so the webpages you visit work correctly. However, at the end of your InPrivate Browsing session, this information is discarded. The following table describes which information InPrivate Browsing discards when you close the browser and how it is affected during your browsing session:

- ▶ **Cookies:** Kept in memory so pages work correctly, but cleared when you close the browser.
- ▶ **Temporary Internet files:** Stored on disk so pages work correctly, but deleted when you close the browser.
- ▶ **Webpage history:** This information is not stored.
- ▶ **Form data and passwords:** This information is not stored.

- ▶ **Anti-phishing cache:** Temporary information is encrypted and stored so pages work correctly.
- ▶ **Address bar and search AutoComplete:** This information is not stored.
- ▶ **Automatic Crash Restore (ACR):** ACR can restore a tab when it crashes in a session, but if the whole window crashes, data is deleted and the window cannot be restored.
- ▶ **Document Object Model (DOM) storage:** The DOM storage is a kind of “super cookie” web developers can use to retain information. Like regular cookies, they are not kept after the window is closed.

InPrivate doesn't clear any history or information about toolbars or browser extensions that is stored on your computer. To help protect your privacy, Internet Explorer disables all toolbars and extensions by default in an InPrivate Browsing window. If you would prefer to enable specific toolbars and extensions during a browsing session, you can do the following:

1. In Internet Explorer, click **Tools** and then click **Manage Add-ons**.
2. Click **Toolbars and extensions**, click the toolbar or extension you want to use, and then click **Enable**.
3. Click **Close**.

## Parental Controls

If you have children who use your computer, you can take extra steps to make sure that they are protected when using Internet Explorer. As mentioned in Chapter 3, Windows 7 offers Parental Controls that enable parents to control browsing behavior in order to help keep children safer online. A child's browsing session can even be examined by a parent afterward, and it cannot be removed without the parent's permission. You can configure Parental Controls from the User Accounts and Family Safety section of Control Panel.

## Certificates for Secure Websites

When you visit a website that begins with https, you are visiting a secure website. Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server. Secure Sockets Layer (SSL) is a protocol for transmitting private documents via the Internet. SSL uses a



cryptographic system that uses two keys to encrypt data—a public key known to everyone and a private or secret key known only to the recipient of the message. Internet Explorer supports SSL and many websites use the protocol to obtain confidential user information, such as credit card numbers.

Certificates provide website identification and encryption for secure connections, as shown in Figure 13.6. If you open Internet Options and click the Content tab, you can remove personal security information that is stored when you use a smart card or public computer kiosk by clicking the **Clear SSL state** button. You can also view or manage the certificates that are installed on your computer by clicking the **Certificates and Publishers** button.

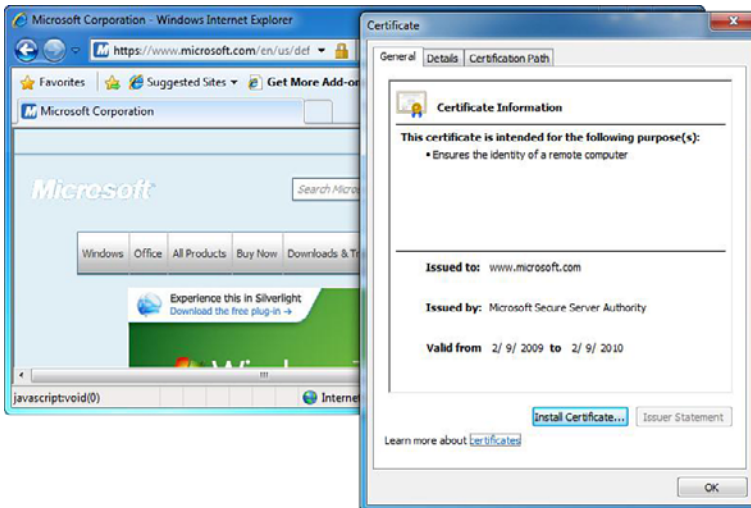


FIGURE 13.6 Digital certificate viewed in Internet Explorer.

## Using Offline Mode and Saving Webpages

You can configure Internet Explorer to view webpages while you are not connected to the network or web server. To enable a website to be offline, you just add your website to your favorites while selecting the Make available offline option.

You can also save a webpage as a file so that you can access it at a later time. To save a webpage, do the following:

1. Go to the webpage you want to save.
2. Click the **Page** button and then click **Save As**.
3. Navigate to the folder where you want to save the webpage.
4. Type a new name in the File name box if you want to change the name.
5. In the Save as type box, do one of the following:
  - ▶ To save all the files associated with the page, including graphics, frames, and style sheets in their original format, click **Webpage, complete**.
  - ▶ To save all information as a single file, click **Web Archive, single file (\*.mht)**.
  - ▶ To save just the current HTML page, without graphics, sounds, or other files, click **Webpage, HTML only**.
  - ▶ To save just the text from the current webpage, click **Text File**.
6. Click **Save**.

Lastly, you can also highlight most webpages or content on a webpage, right-click the highlighted area, and copy the content to the clipboard. You can then paste it into Microsoft Word, WordPad, or some other program.

## RSS Feeds

RSS, short for RDF Site Summary or Rich Site Summary, is an XML format for syndicating web content. A website that wants to allow other sites to publish some of its content creates an RSS document and registers the document with an RSS publisher. A user who can read RSS-distributed content can use the content on a different site. Syndicated content includes such data as news feeds, events listings, news stories, headlines, project updates, excerpts from discussion forums, or even corporate information.

A feed can have the same content as a webpage, but it's often formatted differently. When you subscribe, Internet Explorer automatically checks the website and downloads new content so you can see what is new since you last visited the feed.

To see if a webpage has a feed, the Feeds button changes color, letting you know that feeds are available on the webpage. To subscribe to a feed, do the following:

1. Open **Internet Explorer**.
2. Go to the website that has the feed you want to subscribe to.
3. Click the **Feeds** button to discover feeds on the webpage.
4. Click a feed (if more than one is available). If only one feed is available, you go directly to that page.
5. Click the **Subscribe to this Feed** button and then click **Subscribe to this Feed**.
6. Type a name for the feed and select the folder to create the feed in.
7. Click **Subscribe**.

To view feeds, go to the Feed tab in the Favorites Center. To view your feeds, click the **Favorites Center** button and then click **Feeds**. You can also use other programs, such as email clients like Microsoft Outlook and Windows Sidebar, to read the feeds set up with Internet Explorer. To configure how often feeds are updated or if a sound is played when a feed is found, open Internet Options, select the **Content** tab, and click the **Settings** button.

## Reset Internet Explorer to Default Settings

To reset Internet Explorer settings and to help troubleshoot problems, you can remove all changes that have been made to Internet Explorer since it was installed without deleting your favorites or feeds. To reset Internet Explorer, do the following:

1. Close all Internet Explorer or Windows Explorer windows.
2. Click to open **Internet Explorer**.
3. Click the **Tools** button and then click **Internet Options**.
4. Click the **Advanced** tab and then click **Reset**.
5. Click **Reset**.
6. When you are done, click **Close** and then click **OK**.
7. Close Internet Explorer and reopen it for the changes to take effect.

You can also restore the options in the Advanced tab of the Internet Options dialog box by clicking the **Restore Advanced Settings** button on the Advanced tab.

### ExamAlert

To reset Windows Explorer, click on the **Reset** button within the Advanced tab. If you only want to reset the Advanced options, click the **Restore Advanced Settings** button.

## Compatibility View Mode

Websites designed for earlier versions of Internet Explorer might not display correctly in the current version. Often, you can improve how a website looks in Internet Explorer by using Compatibility View.

When you turn on Compatibility View, the webpage you're viewing (and other webpages within the website's domain) are displayed as if you were using an earlier version of Internet Explorer.

If Internet Explorer recognizes a webpage that isn't compatible, you see the Compatibility View button on the Address bar. To turn Compatibility View on or off, click the **Compatibility View** button, or follow these steps:

1. Click to open Internet Explorer.
2. Click the **Tools** button and then click **Compatibility View**.

The website is displayed in Compatibility View until you turn it off or the website is updated to display correctly in the current version of Internet Explorer.

## Using Accelerators

You can use accelerators with text that you select on a webpage to perform such tasks as opening a street address in a mapping website or looking up the dictionary definition for a word. You can also choose the web services or websites that accelerators use to handle different types of tasks. Internet Explorer comes with a selection of accelerators included by default, but you can add or remove them as you like.

When you first start Internet Explorer, you can accept a selection of default accelerators, or you can choose your own from an online list of accelerators.

The list of new accelerators is frequently updated, so be sure to check back from time to time.

To use an accelerator, follow these steps:

1. Click to open **Internet Explorer**.
2. Go to the webpage that contains the text that you want to use with an Accelerator and select the text.
3. Click the **Accelerator** button to display a list of Accelerators.

If you rest your mouse pointer over each accelerator, you see a preview of the information or content. In many cases, the preview tells you what you want to know, such as a word definition or translation. If not, click the accelerator and Internet Explorer opens the web service using the text you've highlighted.

You can also use an accelerator from the new tab page with text you've copied to the Clipboard, such as from an email message or word-processing document. For example, if you receive a street address in an email that you want to get directions for, you can copy the address to the Clipboard, open Internet Explorer, and open a new tab. On the new tab page, under Use an accelerator, click **Show copied text** if you want to check the text you copied and then click the accelerator you've chosen for mapping.

Although Internet Explorer comes with a selection of accelerators to get you started, you might want to take a look at some of the other accelerators that are available. To find new accelerators, follow these steps:

1. Click to open **Internet Explorer**.
2. Click the **Tools** button and then click **Manage Add-ons**.
3. In Manage Add-ons, under Add-on Types, click **Accelerators** to display a list of your current Accelerators.
4. At the bottom of the screen, click **Find More Accelerators**.
5. On the Internet Explorer Gallery webpage, click the accelerator you want to install and then click **Install Accelerator**.
6. In the Add Accelerator dialog box, do one of the following:
  - ▶ If you're adding a new accelerator, click **Add**. When you add an accelerator, you can also select the **Make this my default provider for this Accelerator Category** checkbox.

- ▶ If you're replacing an existing Accelerator, click **Replace**.
- ▶ If you're not sure you trust the website listed in the From field, click **Cancel**.

## Search Providers

By default, the Instant Search box found in Internet Explorer enables users to perform searches using Microsoft's Bing engine. However, you can add other search engines such as Google and Webopedia to quickly use these services to find what you are looking for.

To add search providers to the Instant Search List, do the following:

1. Open **Internet Explorer**.
2. Click the down arrow on the right side of the Instant Search box and then, from the context menu, select **Find More Providers**.
3. Click the **Add to Internet Explorer** button for one of the Web Search or Topic Search providers.
4. If you want the selected provider to replace Bing as the IE default, select the **Make this my default search provider** checkbox. If you want the provider to provide suggestions as you type searches, select the **Use search suggestions from this provider** checkbox. Then click **Add** to add the selected provider to the Instant Search list.
5. To add a search provider that does not appear on the page, click the **Create your own search provider** link at the bottom of the page to open the Create your own search provider page.

---

## Cram Exam

1. How can you configure IE to automatically delete temporary Internet files when you close Internet Explorer?
  - A. Modify the properties of the Recycle Bin
  - B. Modify the security level of the Internet zone
  - C. Create a script and execute it with Task Scheduler
  - D. Modify the advanced settings from the Internet Options

2. You have a website that appears not to display properly. What can you do for the website to display properly?
- A. Enable an accelerator
  - B. Enable a SmartScreen Filter
  - C. Enable Compatibility View
  - D. Enable a RSS feed
3. What do you use that helps prevent applications from being installed when visiting a website?
- A. InPrivate Browsing
  - B. Protected mode
  - C. Enable Parental Control
  - D. Enable Compatibility View

## Cram Exam Answers

1. **D** is correct. If you go into Advanced settings from Internet Options, you can configure IE to automatically delete their temporary files. Answer A is incorrect because the Recycle Bin is a temporary place to hold delete files. It does not actually delete files. Answer B is incorrect because configure zones do not delete temporary files. Answer C is incorrect because you cannot configure the Task Scheduler to delete temporary files when you close Internet Explorer.
2. **C** is correct. Websites designed for earlier versions of Internet Explorer might not display correctly in the current version. Often, you can improve how a website looks in Internet Explorer by using Compatibility View. Answer A is incorrect because an accelerator is a form of selection-based search that enables a user to invoke an online service from any other page using only the mouse. Answer B is incorrect because a SmartScreen Filter includes protection from socially engineered malware, which helps identify sites that have been labeled as an imposter or harmful (in other words, phishing). Answer D is incorrect because RSS enables a user to read RSS-distributed content on a different site using IE.
3. **B** is correct. Internet Explorer's protected mode is a feature that makes it more difficult for malicious software to be installed on your computer. In addition, it enables users to install wanted software when they are logged in as a standard user instead of an administrator. Answer A is incorrect because the InPrivate Browsing enables you to surf the Web without leaving a trail in Internet Explorer. Answer C is incorrect because parental control is used to help keep children safer online, including restricting websites inappropriate for children. Answer D is incorrect because Compatibility View is used to allow websites that do not display correctly in Internet Explorer 8.
-

# Review Questions

1. You work as the desktop support technician at Acme.com. How do you reset Internet Explorer to its original settings?
  - A. Reinstall Internet Explorer 8.0
  - B. Navigate to the Security tab in Internet Options and click Reset all zones to default level
  - C. Navigate to the Advanced tab in Internet Options and click Restore advanced settings
  - D. Navigate to the Advanced tab and click **Reset**
2. You work as the desktop support technician at Acme.com. How do you remove the stored passwords from a computer?
  - A. On the Security tab in Internet Options, set the Internet zone security to High.
  - B. On the Privacy tab in Internet Options, set the level to Medium.
  - C. On the Privacy tab in Internet Options, set the level to High.
  - D. Navigate to the Advanced tab in Internet Options and click Restore advanced settings.
  - E. Click Tools in the Internet Explorer and then click Delete Browsing History. Click Delete passwords.
3. How do you prevent passwords from being stored locally when visiting websites that require usernames and passwords?
  - A. On the Security tab in Internet Options, set the Internet zone security to High.
  - B. On the Privacy tab in Internet Options, set the level to Medium
  - C. On the Privacy tab in Internet Options, set the level to High.
  - D. On the Content tab in Internet Options, click the AutoComplete Settings button and clear the Usernames and passwords on forms checkbox.
  - E. Click Tools in the Internet Explorer and then click Delete Browsing History. Click Delete passwords.
4. You have a user who is complaining that the images shown in Internet Explorer are too small. What do you need to do?
  - A. You need to decrease the screen resolution.
  - B. You need to increase the screen resolution.
  - C. You need to decrease the zoom level for the tab.
  - D. You need to increase the zoom level for the tab.



5. You work as part of the IT support staff at Acme.com. You have a user that saves files that she downloads from various websites. You want to make sure that when she visits these websites that those websites don't modify those files that she saved previously. What do you need to do?
- A. Disable all ActiveX controls that are currently loaded
  - B. Enable the Phishing Filter
  - C. Change the security level for the Internet zone to High
  - D. Enable Protected Mode option
6. You work as the desktop support technician at Acme.com. When a user clicks a link in a website, nothing happens. What do you think the problem is?
- A. You need to enable an Add-on that the link points to.
  - B. You need to open the Internet Options dialog box. On the Security tab, add the URL to the Trusted sites list.
  - C. You need to open the Pop-up Blocker Settings dialog box. Add the URL to the Allowed sites list.
  - D. You need to open the Internet Options dialog box. On the Privacy tab, add the URL to the Allowed sites list.
  - E. You need to open the Internet Options dialog box. On the Advanced tab, choose the Disable Phishing Filter option.
7. What technology in Internet Explorer is used to protect you from spoofed sites that might try to trick you into divulging confidential information?
- A. Protected mode
  - B. Phishing filter
  - C. Junk mail filter
  - D. Fake Site filter
8. What can be done to notify you when a website has changed?
- A. Configure autoupdate within IIS.
  - B. Configure dynamic update with IIS.
  - C. If a website supports RSS, configure an RSS feed.
  - D. Close Internet Explorer and restart it.
9. You want to delete your cookies and temporary files used by Internet Explorer. You open up Internet options. Which tab enables you to accomplish this?
- A. General tab
  - B. Security tab
  - C. Privacy tab
  - D. Connections tab

10. Which of the following does InPrivate Browsing do? (Choose all that apply.)
- A. Clear out all cookies
  - B. Delete temporary files
  - C. Prevent the storage of form data and passwords
  - D. Enable anti-phishing technology

## Review Question Answers

1. Answer **D** is correct. To reset Internet Explorer to its original settings, navigate to the Advanced tab and click Reset. Answer A is incorrect because reinstalling Internet Explorer does not generally overwrite the settings that are already configured. Answer B is incorrect because resetting zones only affects information specified in the security zones. Answer C is incorrect because this only resets the Advanced options.
2. Answer **E** is correct. To delete saved passwords in Internet Explorer, you must delete the browsing history. Answers A, B, and C are incorrect because these do not affect any saved passwords. Answer D is incorrect because passwords are not stored with the Advanced settings.
3. Answer **D** is correct. To prevent passwords from being stored, you have to configure AutoComplete. Answers A, B, and C do not affect AutoComplete and passwords. Answer E is used to delete saved passwords.
4. Answer **D** is correct. When you have trouble seeing an image, you can use the zoom feature. Answers A and B are incorrect because they affect all programs. Answer C is incorrect because decreasing the zoom makes the image smaller.
5. Answer **D** is correct. Protected mode helps protect you from websites that try to save files or install programs on your computer. Answer A is incorrect because disabling all ActiveX components might disable functionality that you might use for other websites. Answer B is incorrect because the phishing filter is used to stop users from being tricked into fake sites that emulate corporate sites in an attempt to steal confidential information. Answer C might or might not affect the control, but it is never stated what level the website is.
6. Answer **B** is correct. When you click some links, the links open separate windows. If you have a pop-up blocker set up, the site might be blocked. Answer A is incorrect because add-ons are designed to run within a website, not as a standalone application. Adding a URL to a trusted site might have some effect on functionality, but it does not allow or disallow the entire window for opening. Answers C and D are incorrect because neither of these affect whether a website opens.

7. Answer **B** is correct. Some sites are created to look as other sites and are used to lure people to divulge confidential information. Because these sites are “fishing” for information, these sites are referred to as *phishing*. Answer A is incorrect because protected mode tries to secure the Internet Explorer by securing other files. Answer C is incorrect because a junk mail filter is used in email. Answer D is incorrect because there is no such thing as a fake site filter.
8. Answer **C** is correct. RSS feeds are used to get automatic updates and notifications when a website posts something new. Answer B is incorrect because dynamic updates are a set of technology to help protect your system when using Internet Explorer. Answer A is incorrect because configuring autoupdate within IIS is used to automatically update Windows security patches and fixes. Answer D is incorrect because closing Internet Explorer and restarting opens up the home page again. It does not notify when other websites get updated.
9. Answer **A** is correct. The General tab is where you can delete temporary files, history, cookies, saved passwords and web form information. Answer B is incorrect because the Security tab is where you configure the security zones. Answer C is incorrect because the Privacy tab is used to configure the use of cookies and to enable or disable the pop-up blocker. Answer D is incorrect because the Connections tab is used to configure IE to use a proxy server or an Internet connection.
10. Answers **A**, **B**, and **C** are correct. InPrivate Browsing (new to IE 8) enables you to surf the Web without leaving a trail in Internet Explorer. This includes clearing out cookies, deleting temporary files, preventing the storage of form data and passwords, and not storing webpage history. Answer D is incorrect because although InPrivate Browsing encrypts and stores the anti-phishing cache, it does not enable or disable anti-phishing technology.

## CHAPTER 14

# Mobile Computers and Remote Management

### **This chapter covers the following 70-680 Objectives:**

- ▶ Configuring Network Connectivity:
  - ▶ Configure remote management
- ▶ Configuring Mobile Computing:
  - ▶ Configure remote connections
  - ▶ Configure mobility options

Mobile computers are computers that are meant to be mobile. Just like desktop computers, mobile computers (including laptops, notebook computers, tablet PCs, and Ultra-Mobile computers) can come in various sizes and configurations. Mobile computers have an inherent set of challenges as they are not always connected to the Internet or corporate offices where they can be managed and they are designed to be portable, to conserve power for a longer battery life, and to run cooler, which usually affect performance.

A mobile device is a computing device that has been optimized for specific mobile computing tasks. Mobile device types include the following:

- ▶ PDAs
- ▶ Windows Mobile devices
- ▶ Portable media players
- ▶ Mobile phones

Mobile devices offer their own challenges because they are often configured to synchronize with a desktop or mobile computer to obtain data.

While you are using mobile computers as well as desktops, you might have a need to remotely connect to and control another computer or server.

Windows 7 offers several tools that enable you to do that, including Remote Desktop, Remote Assistant, and PowerShell.

# Control Panel and Windows Mobility Center

- ▶ **Configure mobility options**
- ▶ **Configure performance settings**

## CramSaver

1. Which of the following do you find in the Mobility Center? (Choose all that apply.)
  - A.** Volume
  - B.** Presentation Settings
  - C.** Display Settings
  - D.** External Display
2. What command would you use to turn off the hibernate function and to remove the hiberfil.sys file?
  - A.** Run the `powercfg -hibernate off` command
  - B.** Open a command prompt and delete the hiberfil.sys file
  - C.** Open the Power settings within the Control Panel and uncheck Enable Hibernate option
  - D.** Run the `Hibernate On` command
3. What application do you use to manage your offline folders?
  - A.** System Configuration tool
  - B.** Offline folder console
  - C.** Sync Center
  - D.** Mobility Share tool

## Answers

1. **A, B, and D** are correct. The Mobility Center includes Volume, Battery Status, Wireless Network, External Display, Sync Center, Presentation Settings, and Screen Rotation. Because the Display Settings are not listed, Answer C is incorrect as you cannot modify your display settings from the Mobility Center.

2. **A** is correct. The `powercfg` command is a command-line tool that enables you to control the power settings on a system. To disable hibernate and remove the `hiberfil.sys` file, you use the `powercfg -hibernate` command. Answer B is incorrect because deleting the `hiberfil.sys` command does not disable hibernate. Answer C is incorrect because there is no Enable Hibernate option. Answer D is incorrect because there is no `Hibernate On` command.
3. **C** is correct. When you set up the synchronization, you may set up a one-way or two-way synchronization. To configure Offline Files, click Open the Sync Center and then click Manage offline files. Answer A is incorrect because the System Configuration tool is a tool to troubleshoot startup problems. Answers B and D are incorrect because there is neither an Offline folder console nor a Mobility Share tool.

All mobile and power settings are configured within the Control Panel. To make finding these settings quick and easy, Windows 7 includes the Windows Mobility Center, which provides a single location that enables you to quickly adjust mobile PC settings, as shown in Figure 14.1. Depending on your system, the Mobility Center window has some, but perhaps not all, of the following tiles:

- ▶ **Volume:** Move the slider to adjust the speaker volume of your mobile PC or select the Mute check box
- ▶ **Battery Status:** View how much charge remains on your battery or select a power plan from the list
- ▶ **Wireless Network:** View the status of your wireless network connection or turn your wireless adapter on or off
- ▶ **External Display:** Connect an additional monitor to your mobile PC or customize the display settings
- ▶ **Sync Center:** View the status of an in-progress file sync, start a new sync or set up a sync partnership, and adjust your settings in Sync Center
- ▶ **Presentation Settings:** Adjust settings, such as the speaker volume and the desktop background image, for giving a presentation
- ▶ **Screen Rotation:** Change the orientation of your Tablet PC screen, from portrait to landscape, or vice versa

If a tile doesn't appear, it might be because the required hardware, such as a wireless network adapter, or drivers are missing.

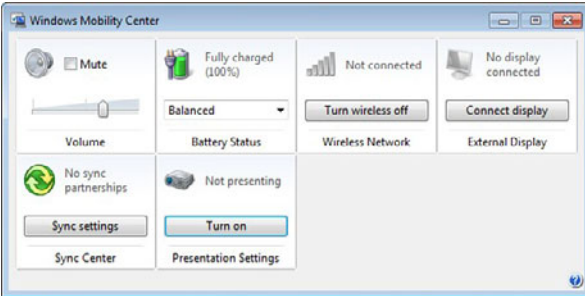


FIGURE 14.1 Windows Mobility Center.

If you need to make additional adjustments to your mobile PC settings that require you to access Control Panel, click the icon on a tile to open Control Panel for that setting. For example, you can select an existing power plan from the Battery Status tile, or you can click the icon on the tile to open Power Options in Control Panel to create a power plan.

The Mobility Center can be opened using any one of the following methods:

- ▶ Click the **Start** button, click **Control Panel**, click **Mobile PC**, and then click **Windows Mobility Center**.
- ▶ Click the battery meter icon in the notification area in the Windows taskbar, and then click **Windows Mobility Center**.
- ▶ Press the **Windows logo key + X**.

## Configuring Presentation Settings for Mobile PCs

Presentation settings are options on your mobile PC that you can apply when giving a presentation. If you've ever had your display screen turn black during a presentation, you'll appreciate that you can automatically turn off your screen saver every time that you give a presentation.

When presentation settings are turned on, your mobile PC stays awake and system notifications are turned off. You can also choose to turn off the screen saver, adjust the speaker volume, and change your desktop background image. Your settings are automatically saved and applied every time that you give a presentation, unless you manually turn them off.

You can turn on presentation settings by using one of the following methods:

1. Open the Windows Mobility Center by clicking the **Start** button, clicking **Control Panel**, clicking **Mobile PC**, and then clicking **Windows Mobility Center**.
2. On the Presentation Settings tile, click **Turn on**.
3. Click **OK**.

To turn presentation settings on or off for the current monitor or projector that the mobile PC is connected to, follow these steps:

1. Open Windows Mobility Center by clicking the **Start** button, clicking **Control Panel**, clicking **Mobile PC**, and then clicking **Windows Mobility Center**.
2. On the Presentation Settings tile, click the **Change Presentation Settings** icon to generate the window in Figure 14.2.
3. In the Presentation Settings dialog box, click **Connected displays**.
4. In the Current Displays dialog box, select or clear the **I always give a presentation when I use this display configuration** checkbox, and then click **OK**.

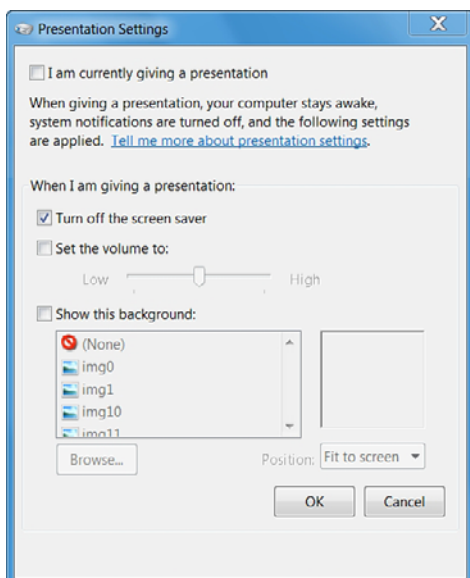


FIGURE 14.2 Changing Presentation settings.



Presentation settings automatically turn off when you disconnect your mobile PC from a network projector or additional monitor, and when you shut down or log off from your mobile PC. Or, you can manually turn off presentation settings:

1. Open Windows Mobility Center by clicking the **Start** button, clicking **Control Panel**, clicking **Mobile PC**, and then clicking **Windows Mobility Center**.
2. On the Presentation Settings tile, click **Turn off**.

To customize presentation settings:

1. Open Windows Mobility Center by clicking the **Start** button, clicking **Control Panel**, clicking **Mobile PC**, and then clicking **Windows Mobility Center**.
2. On the Presentation Settings tile, click the **Change Presentation Settings** icon.
3. In the Presentation Settings dialog box, adjust settings for giving a presentation and then click **OK**.

To keep the display on during presentations:

1. Open Windows Mobility Center by clicking the **Start** button, clicking **Control Panel**, clicking **Mobile PC**, and then clicking **Windows Mobility Center**.
2. On the Presentation Settings tile, click the **Change Presentation Settings** icon.
3. Expand **Display**, expand **Turn off display after**, click **On battery or Plugged in**, and then click the arrow to change the setting to **Never**. You can also type the word **never** in the box.
4. Click **OK** and then click **Save changes**.

To prevent the mobile PC from going to sleep during presentations:

1. Open Windows Mobility Center by clicking the **Start** button, clicking **Control Panel**, clicking **Mobile PC**, and then clicking **Windows Mobility Center**.
2. On the Presentation Settings tile, click the **Change Presentation Settings** icon.

3. Expand **Sleep**, expand **Sleep after**, click **On battery** or **Plugged in**, and then click the arrow to change the setting to **Never**. You can also type the word **Never** in the box.
4. Click **OK** and then click **Save changes**.

## Power Management

One of the goals of mobile computers is to run off the battery for as long as possible. Therefore, the mobile computers use components that typically use less power than components that you would find in a desktop computer. For example:

- ▶ Mobile computers use processors that run on a lower voltage and consume less power.
- ▶ Mobile processors, including Intel SpeedStep and AMD PowerNow, have the capability to adjust voltage and the capability to throttle (temporarily run at a slower clock speed) to use even less power when running off the battery.
- ▶ LCD monitor can be dimmed so that it consumes less power.
- ▶ Mechanical Hard drives can be spun down when not in use.

### Note

Although Solid State Drives (SSD) are based on a relatively new technology, SSDs are starting to replace traditional mechanical devices. Because Solid State Drives do not contain mechanical parts, they consume less power, allowing for a longer battery life.

## Power Plans

A power plan (formerly known as a power scheme in earlier versions of Windows) is a collection of hardware and system settings that manages how your computer uses and conserves power. You can use power plans to save energy, maximize system performance, or balance energy conservation with performance.

Windows 7 includes three default power plans, as shown in Figure 14.3:

- ▶ **Balanced:** Offers full performance when you need it and saves power during periods of inactivity.

- ▶ **Power saver:** Saves power by reducing system performance. This plan can help mobile PC users get the most from a single battery charge.
- ▶ **High performance:** Maximizes system performance and responsiveness. Mobile PC users might notice that their battery doesn't last as long when using this plan.

If a default plan doesn't meet your needs (even if you change some settings), you can create your own plan by using a default plan as a starting point.

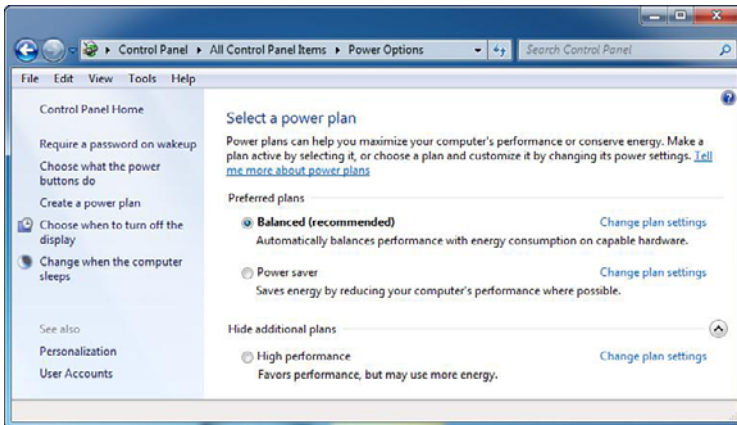


FIGURE 14.3 Configuring power plans using the Control Panel.

To change an existing plan, do the following:

1. Open Power Options by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **Power Options**.
2. On the Select a power plan page, click **Change plan settings** under the plan that you want to change.
3. On the Change settings for the plan page, choose the display and sleep settings that you want to use when your computer is running on battery and when it's plugged in.
4. If you don't want to change any more settings, click **Save changes**. To change additional power settings, click **Change advanced power settings**.

5. On the Advanced settings tab, expand the category that you want to customize, expand each setting that you want to change, and then choose the values that you want to use when your computer is running on battery and when it's plugged in.
6. Click **OK** to save the changes and then click the **Close** button on the Change settings for the plan page.

To create your own plan, use the following steps:

1. Open Power Options by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **Power Options**.
2. On the Select a power plan page, in the task pane, click **Create a plan**.
3. On the Create a power plan page, select the plan that's closest to the type of plan that you want to create.
4. In the Plan name box, type a name for the plan and then click **Next**.
5. On the Change settings for the plan page, as shown in Figure 14.4, choose the display and sleep settings that you want to use when your computer is running on battery and when it's plugged in and then click **Create**.

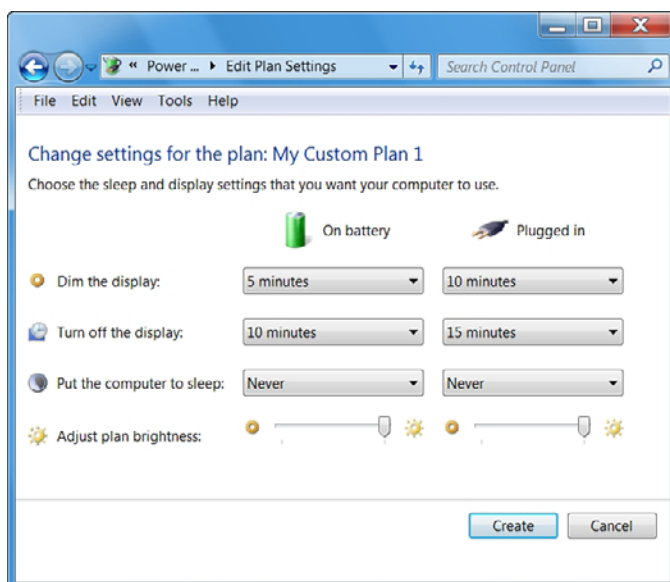


FIGURE 14.4 Changing settings for a power plan.

If you created power plans that you no longer use or need, you can delete them. To delete a plan, do the following:

1. Open Power Options by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **Power Options**.
2. If the active plan is the one that you want to delete, make a different plan the active plan.
3. On the Select a power plan page, click **Change plan settings** under the plan that you want to delete.
4. On the Change settings for the plan page, click **Delete this plan**.
5. When prompted, click **OK**.

#### Note

You can't delete any of the three default power plans (Balanced, Power saver, or High performance).

## Shut Down Options

When you shut down your computer, all open files are saved to the hard disk, the contents of the memory are saved to the hard disk or discarded as appropriate, the page file is cleared, and all open applications are closed. The active user is then logged out of Windows and the computer is turned off. Of course, this might take a minute or two, depending on the computer and the applications that the computer was running at the time of shutdown.

Windows 7 offers two other modes besides shutdown. When you hibernate your computer, the system state, along with the contents of the system memory, is saved to a file (hiberfil.sys) on the hard disk and the computer is shut down. The hiberfil.sys file is same size as the amount of physical memory (RAM). No power is required to maintain this state because the data is stored on the hard disk. You can then continue where you left off within a short time.

Sleep is a power-saving state that saves work and open programs to memory. To maintain the contents of memory while the computer is in sleep mode, the system still consumes a small amount of power. The advantage of Sleep mode is that you can continue where you left off, typically within a few seconds.

Hybrid sleep, a combination of sleep and hibernate, saves your work to your hard disk and puts your mobile PC into a power-saving state. If you suffer a

power failure on a computer when it is in a hybrid sleep state, your data is not lost. Hybrid sleep is turned off by default on mobile PCs.

When you click the power button on the Start menu, Windows 7 automatically goes into Sleep mode. If your battery power is low, Windows 7 hibernates the computer.

In addition to power plans, you can configure what the computer does when you press the power button or when you close the lid (on a laptop computer), as shown in Figure 14.5. You can also tell Windows 7 whether to prompt for a user password when returning to its power-on state. You can also control button actions depending on whether the computer is plugged in or running on battery power.

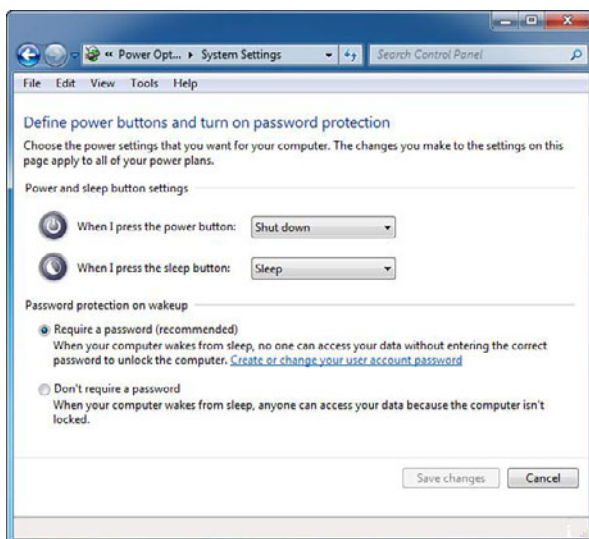


FIGURE 14.5 System settings for power, sleep buttons, and lid settings.

By default, hibernate is enabled. If you want to disable hibernate and remove the hiberfil.sys file on the C drive, you use the following command:

```
powercfg -hibernate off
```

## Battery Meter

Displayed in the notification area of the Windows taskbar, the battery meter helps you manage your computer's power consumption by indicating how much charge is remaining on your battery and which power plan your computer is using.

Windows continuously monitors the power level of your battery and warns you when the battery power reaches low and critical levels. When your battery charge gets low, the battery icon on the Windows taskbar indicates a low-battery power level. Make sure that you have sufficient time to install a fully charged battery, find an AC power outlet, or save your work and turn off the mobile PC. When your battery is almost out of power, the battery icon changes to indicate a critical-battery level.

To choose low and critical power levels, do the following:

1. Open Power Options by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then clicking **Power Options**.
2. On the Select a power plan page, click **Change plan settings** under the selected plan.
3. On the Change settings for the plan page, click **Change advanced power settings**.
4. On the Advanced settings tab, expand **Battery**, expand **Low battery level** and **Critical battery level**, and then choose the percentage that you want for each level.
5. Click **OK** to save the changes and then click the **Close** button on the Change settings for the plan page.

## File and Data Synchronization

While using mobile computers, sometimes you are connected to a corporate network and other times you are not. Sometimes you might want to work on the files stored on a network server even when you are not connected to the network that holds the network server. You might also want to connect mobile devices such as phones and PDAs to your mobile computer or desktop computer so that information can be copied back and forth.

The Windows 7 Sync Center provides a single easy-to-use interface to manage data synchronization between multiple computers including network servers and with mobile devices you connect to your computer. To start the Sync Center, click the **Start** button, click **All Programs**, click **Accessories**, and then click **Sync Center** to generate the screen shown in Figure 14.6.

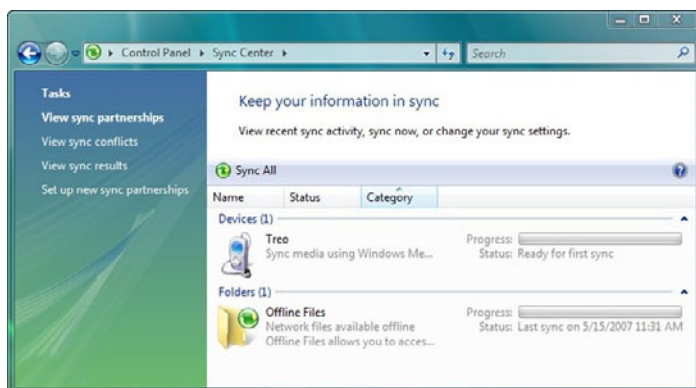


FIGURE 14.6 Sync Center.

To set up synchronization between two computers, you create a sync partnership between two or more sync locations, which specifies what files and folders to sync, where to sync them, and when. You can schedule an automatic sync on a daily, weekly, or monthly basis, or when a specific event occurs, such as every time you log on to your computer. You can also perform a manual sync at any time, such as when you are getting ready to disconnect a mobile PC from the network and want to make sure you have the latest copies of files on a network server.

### Note

The ability to sync with network folders is not included in Windows 7 Starter, Windows 7 Home Basic, or Windows 7 Home Premium.

Every time you sync files between two locations (such as between a computer and a mobile device), Sync Center compares the files in both locations to see if they still match or if any have changed. It determines if any files need to be updated in order to stay in sync.

If the files differ, Sync Center determines which version of each file to keep and copies that version to the other location, overwriting the other version there. It selects the most recent version to keep, unless you have set up the sync partnership to sync differently. Sometimes, Sync Center prompts you to choose which version of a file to keep. This usually occurs when a file has changed in both locations since the last sync. When this happens, Sync Center notifies you of a sync conflict, which you must resolve before it can sync the items in conflict.



When you set up the synchronization, you may set up a one-way or two-way synchronization. In one-way sync, files are copied from a primary location to a secondary location, but no files are ever copied back to the primary location. In two-way sync, Sync Center copies files in both directions, keeping the two locations in sync with each other. Most sync partnerships are automatically set up to perform either one-way or two-way sync, although some sync partnerships let you choose.

You might set up two-way sync between a network folder and your computer, where you instruct Sync Center to copy the newest version of any file it finds to the other location, overwriting any older versions of the same file. This is a good way to sync if you work with the same files on both the network folder and your computer, and you want to make sure you always have the most recent version of every file you've worked on.

You might set up one-way sync for a portable music player, for example, where you instruct Sync Center to copy every new music file from your computer to the mobile device but never to copy music files in the other direction (from the device to your computer).

## Offline Folders

Because many users use portable computers many users have a need to access files in a shared folder while not being connected to the network where the shared folder is. To overcome this problem, you can use offline files.

To configure Offline Files, click **Open the Sync Center** and then click **Manage offline files**. From the General tab in the Offline Files dialog box, you can enable or disable offline files by clicking the top button. You can also use the General tab to open Sync Center and to view your offline files, as shown in Figure 14.7.

The Disk Usage tab enables you to see how much disk space is currently being used by offline files and enables you to change the limits of storage that offline uses. The Encryption tab enables you to encrypt or decrypt your offline files.

The Network tab enables you to choose to automatically work on any locally cached offline files when your connection to the network is slow. You can also choose how often to check for a slow network connection.

In addition, you can encrypt your offline files to help secure private information using the Sync Manager. Of course, when you encrypt offline files, only your user account can access the cached data.

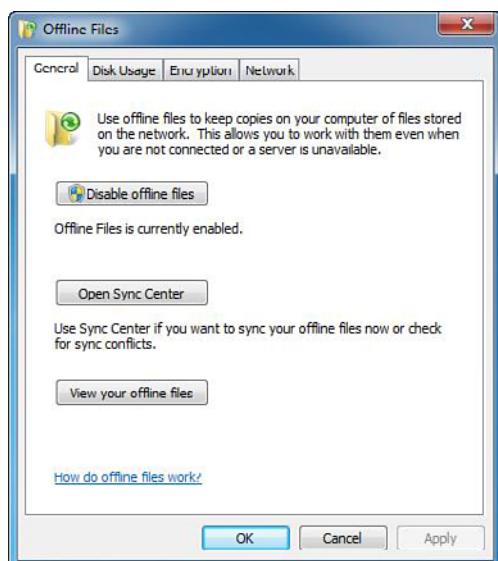


FIGURE 14.7 Offline Files options.

After a folder is shared, you can control if a folder is available as an offline folder and how remote users access files inside each of your shares. The Caching settings for shared folders are configured by clicking the **Advanced Sharing**, on the Sharing tab of the folder's property sheet and clicking the **Caching** button to generate the resulting window in Figure 14.8. The options are as follows:

- ▶ **Only the files and programs that users specify will be available offline:** This setting is the default and enables any files or programs in the share to be available offline to users but users must make the decision.
- ▶ **No files or programs from the shared folder are available offline:** This setting disables caching from the share.
- ▶ **All files and programs that users open from the share will be automatically available offline:** This setting ensures that any files a user accesses from this share while online are available offline.
- ▶ **Optimized for performance:** This checkbox enables the caching to take place in the background, therefore helping to optimize network performance.

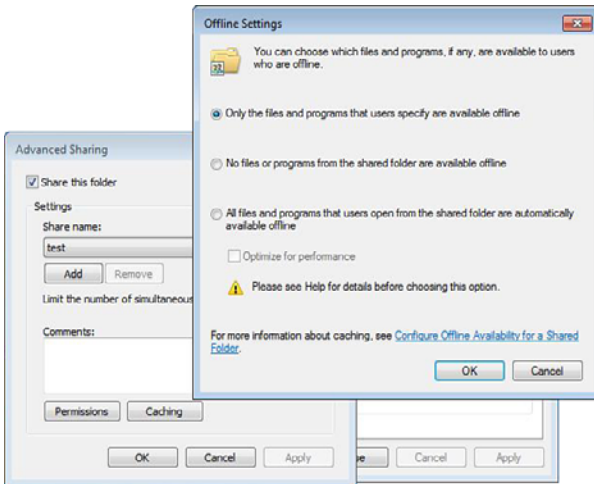


FIGURE 14.8 Caching options.

To make files or folders available offline, do the following:

1. While connected to the network, locate the network file or folder that you want to make available offline.
2. Right-click the file or folder and then click **Always available offline**.

Windows automatically creates a copy of that file or folder on your computer. Anytime you reconnect to that network folder, Windows syncs the files between your computer and the network folder. You can also sync them manually at any time.

If you work with offline files in different folders, you might want to view all of them without opening each folder individually. To enable this functionality, do the following:

1. Open the **Sync Center**.
2. Click the **Manage offline files** option.
3. On the General tab, click **View your offline files**.

If you want to sync your offline files right away to be sure you have the latest versions of files stored on the network, do the following:

1. Click to open **Sync Center**.
2. Click the **Offline Files** folder. Then, on the toolbar, click **Sync** to sync all your offline files.

If you want to sync only one file or folder, or a selection of files, you don't need to open Sync Center. Simply right-click the item, point to Sync, and then click **Sync selected offline files**.

## Connecting Mobile Devices

Many mobile devices can connect to your Windows 7 computer and synchronize data and files between the two. Typically, you connect your device to your computer either using a USB cable or cradle or through a wireless signal (infrared, Bluetooth, or Wi-Fi). Most devices ship with a USB cable or cradle, and most modern computers are equipped with infrared or Bluetooth.

If you are connecting a mobile device using Bluetooth technology, you need to configure that the device is discoverable. You also need to set up the passkey to associate the device with the Bluetooth signal. This ensures that each device is connected to the device to which it is intended to connect.

### ExamAlert

You can use the Windows Mobility Device Center to disable USB connections and Bluetooth connections. You can access Mobility Device Center by opening the Control Panel, clicking Mobile PC, and selecting Mobility Device Center.

Before you can synchronize information with devices, you must set up sync partnerships. To create a sync partnership with a portable media player, you just need to do the following:

1. Connect your device to a computer running Windows 7 and open Sync Center. Windows 7 includes drivers for many common devices, but you can also obtain drivers from the CD that came with your device or from Windows Update.
2. Set up a sync partnership. Clicking **Set up for a media device sync partnership** opens Windows Media Player 11.
3. Select some media files or a playlist to synchronize to the device. To select media, simply drag it onto the sync dialog box on the right side of Windows Media Player.
4. Click **Start Sync**. When your chosen media has transferred to the device, you can disconnect it from your computer and close Windows Media Player.

You can sync your contacts with some mobile devices, enabling you to take your contacts with you wherever you go. To sync contacts with a mobile device, the device must be able to read the contact file that Windows creates for each individual contact. The device must also be compatible with Sync Center, which Windows uses to sync files between a computer and a mobile device.

If you have Exchange Server 2003 or later deployed in your organization, take advantage of its integration with Windows Mobile, which provides direct push email using ActiveSync technology, Global Address List lookup, and numerous security features.

## Windows SideShow

Windows SideShow is a new technology in Windows 7 that supports a secondary screen on your mobile PC. With this additional display, you can view important information such as running Windows Media Player or check email whether your laptop is on, off, or in sleep mode. Windows SideShow is available in Windows 7 Home Premium, Windows 7 Professional, Windows 7 Enterprise, and Windows 7 Ultimate.

Windows SideShow uses gadgets, convenient mini programs, to extend information from your computer to other devices. Gadgets can run on a Windows SideShow-compatible device and update that device with information from your computer. Using a gadget, you can view information from your computer regardless of whether your mobile PC is on, off, or in the sleep power state, which can save you both time and battery life.

To configure Windows SideShow, you have to search Windows Help and Support for “Turn on Windows SideShow.” After clicking the **Turn a Windows SideShow gadget on or off**, click the **Click to open Windows SideShow** link to generate the window shown in Figure 14.9. You can then turn gadgets on or off for each of your devices (assuming you have SideShow gadgets). From Control Panel, you can also set your computer to wake periodically (such as every hour) so that all gadgets that are turned on can update your devices with the latest information.

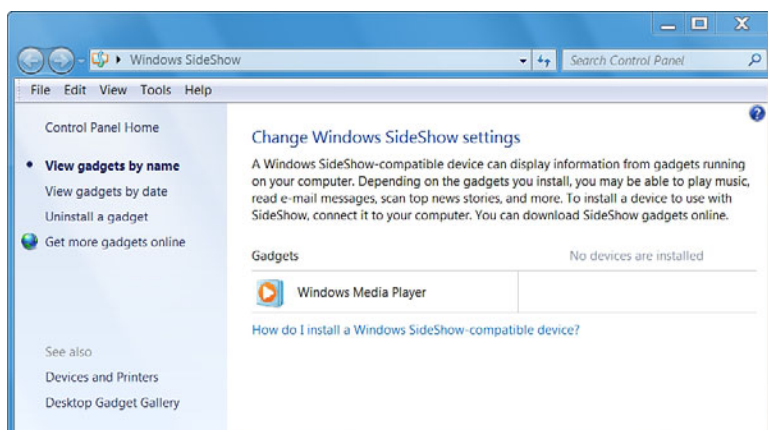


FIGURE 14.9 Windows SideShow.

Windows SideShow-compatible devices can take many forms. Hardware manufacturers are already including secondary displays in their designs for mobile PCs and devices such as keyboards, mobile phones, and remote controls.

## Remote Projector

A network projector is a video projector that's connected to a wireless or wired local area network (LAN). What sets the network projector apart from other presentation methods is that you can connect to, and operate the projector remotely over, a network connection. If your computer can connect to the projector, you can deliver a presentation from any location that has network access, whether it's your private office or a conference room where the projector is located. Those who want to view your presentation must be in the same room as the projector; they can't view the presentation over the network from a different location.

To start, connect to the projector by using one of the following methods:

1. Open the Connect to a Network Projector Wizard by clicking the **Start** button, clicking **All Programs**, clicking **Accessories**, and then clicking **Connect to a Network Projector**.

2. Then do one of the following:
  - a. Click the search for a projector (recommended option). Click the projector you want to connect to and click the Connect button.
  - b. Click **Enter the projector network address** and enter the address as a URL (a web address, such as `http://server/projectors/projector_1`) or as a UNC path (a path on a server, such as `\\server\projectors\projector_1`) and the appropriate password.
3. After you're connected, you can control your presentation in the Network Presentation dialog box by clicking **Pause**, **Resume**, or **Disconnect**.

#### Note

Network projectors are designed to transmit and display still images, such as photographs and Microsoft Office PowerPoint slides—not high-bandwidth transmissions, such as video streams. The projector can transmit video, but the playback quality is often poor.

---

## Cram Quiz

1. You have a folder that you want to make available offline. What do you need to do?
  - A. Share a folder and ensure that the Allow caching of files in this shared folder checkbox is selected
  - B. Map a network drive to the folder and select the cached option
  - C. Use the `cache` command
  - D. Grant the cache permission to the user
2. You are ready to give a presentation using your computer, running Microsoft PowerPoint. What should you do to prepare your system for the presentation? (Choose the best answer.)
  - A. Create a second hardware profile, reboot the computer and load the second hardware profile
  - B. Shut off your email and messengers, change your volume, change your screen, and disable screen savers and sleep features
  - C. Create a second user profile, configure the profile for presentations, and log in as that user to give the presentation
  - D. Configure your Presentation Settings and enable Presentation Settings On

3. Which of the following shutdown option enables you to save the contents of RAM into a file, shut down the system, quickly boot the system, and continue working with the same applications that you had open when you shut down the system?
- A. Sleep
  - B. Hibernate
  - C. Reduced Power mode
  - D. Deep Sleep mode

## Cram Quiz Answers

1. **A** is correct. After you share a folder, make sure that you ensure that the Allow caching of files in this shared folder check box is selected. Answer B is incorrect because when you map a network drive, there is no cached option. Answer C is incorrect because there is no `cache` command. Answer D is incorrect because there is no cache permission.
  2. **D** is correct. The best way to give presentations is to configure Presentation Settings with the Mobility Center and turn the Presentation Settings to On when you are to give a presentation. You could create profiles (user or hardware) but this requires more work and it is not as efficient as using Presentation mode. Therefore, Answers A and C are incorrect. Answer B is incorrect because by changing your settings each time you give a presentation is time consuming and not efficient.
  3. **B** is incorrect. When you hibernate your computer, the system state, along with the contents of the system memory, is saved to a file (Hiberfil.sys) on the hard disk and the computer is shut down. The hiberfil.sys file is the same size as the amount of physical memory (RAM). No power is required to maintain this state because the data is stored on the hard disk. You can then continue where you left off within a short time. Answer A is incorrect because Sleep mode is similar to hibernate but uses a small amount of memory to keep the contents of memory active instead of saving to a file. Answers C and D are incorrect because there is neither a Reduced Power mode nor a Deep Sleep mode.
-



# Remote Desktop and Remote Assistance

- ▶ **Configure remote management**
- ▶ **Configure remote connections**

## CramSaver

1. Which tool would you use to view the desktop of remote user so that you can see the problem as she tries to open a program?
  - A.** Remote Assistance
  - B.** Remote Desktop
  - C.** Computer Management console
  - D.** System Information console
2. You want to view someone's Event Viewer without logging directly onto his computer. What option should you use?
  - A.** System Information
  - B.** Computer Management console
  - C.** System Configuration tool
  - D.** Remote Management console

## Answers

1. **A** is correct. Remote Assistance enables you to view and interact a user's session on a computer running Windows 7 so that you can work with the user to troubleshoot and fix the problem. Answer B is incorrect because Remote Desktop only enables you to log in to a remote computer but not enable you to connect to another user's session. Answer C is incorrect because the Computer Management console enables you to run several Administrative tools from a single console but it does not enable you to view a user's desktop. Answer D is incorrect because the System Information program (not console) enables you to view system information so that you can provide it easily to people troubleshooting problems.
2. **B** is correct. By using Computer Management console, you can connect to remote computers to manage including viewing the Event Viewer. Answer A is incorrect because the System Information is used to view a systems configuration. Answer C is incorrect because the System Configuration tool is used to troubleshoot boot problems. Answer D is incorrect because there is no Remote Management console.

Starting with Windows XP, Microsoft introduced Remote Desktop and Remote Assistance. Similar to Terminal Services used in Windows 2000 servers, you can have access to a Windows session that is running on your computer when you are at another computer. This means, for example, that you can connect your work computer from home and have access to all of your applications, files, and network resources as though you were in front of your computer at work. You can leave programs running at work and when you get home, you can have your desktop at work displayed on your home computer, with the same programs running. Another example of using Remote Desktop and Remote Assistance is to remotely troubleshoot or administer a computer that is not nearby.

While using Remote Desktop and Remote Assistance, you can use your keyboard and mouse just like you are connected to the computer. You can click the **Start** button and click **Windows Security**, you can access the Security Window so that you can log off, reboot the computer, access the Task Manager, or change the password. If for some reason the Explorer taskbar is not available, you can also press the **Ctrl+Alt+End** keys to open the same window.

To use Remote Desktop and Remote Assistance, you have to use TCP port 3389. Therefore, it needs to be opened using the Windows Firewall and any other firewalls between your computer and the remote host.

## Remote Desktop and Remote Desktop Connections

You use Remote Desktop to access one computer from another remotely. With Remote Desktop Connection, you can access a computer running Windows from another computer running Windows that is connected to the same network or to the Internet. For example, you can use all your work computer's programs, files, and network resources from your home computer, and it's just like you're sitting in front of your computer at work.

### ExamAlert

You cannot use Remote Desktop Connection to connect to computers running Windows 7 Starter, Windows 7 Home Basic, Windows 7 Home Premium, and you can only create outgoing connections from those editions of Windows 7. Only Windows 7 Professional, Ultimate, and Enterprise editions support Remote Desktop Hosting.

**Note**

You cannot use Remote Desktop Connection to connect to computers running Windows XP Home Edition.

To connect to a remote computer, it must meet the following criteria:

- ▶ The remote computer must be turned on.
- ▶ The remote computer must have a network connection.
- ▶ Remote Desktop must be enabled.
- ▶ You must have network access to the remote computer (this could be through the Internet).
- ▶ You must have permission to connect (a member of the administrators group or the Remote Desktop Users group. For permission to connect, you must be on the list of users.

**ExamAlert**

To use Remote Desktop, the computer that you are trying to connect to must be on, Remote Desktop must be enabled, and you must have the proper rights.

**Note**

Remote Desktop uses port 3389.

To allow remote connections on the computer you want to connect to, do the following:

1. Click the **Start** button. Right-click **Computer** and select **Properties**.
2. Click **Remote Settings** and then select one of the three options under Remote Desktop, as shown in Figure 14.10. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3. Click **Select Users**. If you are enabling Remote Desktop for your current user account, your name is automatically added to this list of remote users, and you can skip the next two steps.
4. In the Remote Desktop Users dialog box, click **Add**. This adds users to the Remote Desktop Users group.
5. In the Select Users dialog box, do the following:
  - ▶ To specify the search location, click **Locations** and then select the location you want to search.
  - ▶ In Enter the object names to select, type the name of the user that you want to add and then click **OK**.

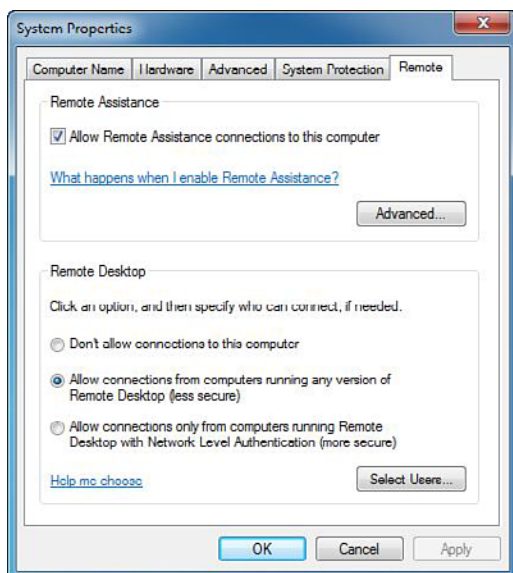


FIGURE 14.10 Remote Assistant and Remote Desktop settings.

The name is displayed in the list of users in the Remote Desktop Users dialog box, as shown in Figure 14.11.

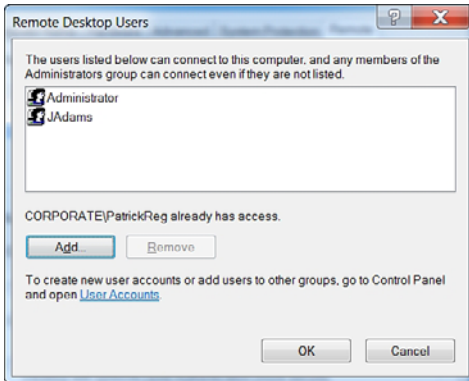


FIGURE 14.11 Adding remote desktop users.

To start Remote Desktop on the computer you want to work from, do the following:

1. Open Remote Desktop Connection by clicking the **Start** button, select **Accessories**, and select **Remote Desktop Connection**.
2. From the screen shown in Figure 14.12, in the Computer field, type the name of the computer that you want to connect to and then click **Connect**. (You can also type the IP address instead of the computer name if you want.)

For more advanced options before the connection, click the **Options** button.

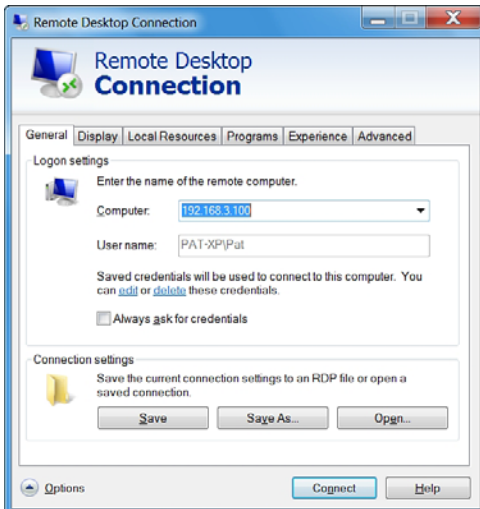


FIGURE 14.12 Using Remote Desktop Connection.

## Using Remote Assistance

Remote Assistance is used to give or receive assistance remotely. For example, a friend or a technical support person can access your computer to help you with a computer problem or show you how to do something. You can help someone else the same way. In either case, both you and the other person see the same computer screen. If you decide to share control of your computer with your helper, you are both able to control the mouse pointer.

To use Remote Assistance, first you invite a person to help you, using email or an instant message, as shown in Figure 14.13. You can also reuse an invitation that you have sent before. After the person accepts the invitation, Windows Remote Assistance creates an encrypted connection between the two computers over the Internet or the network that both computers are connected to. You give the other person a password so that he or she can connect. You can also offer assistance to someone else, and when that person accepts your offer, Windows Remote Assistance creates an encrypted connection between the two computers. To start a Remote Assistance session and to create invitations, click **All Programs**, select **Maintenance**, and select **Windows Remote Assistance**.

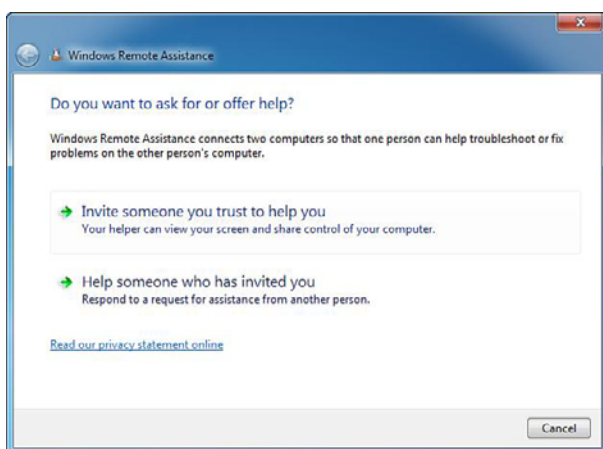


FIGURE 14.13 Remote Assistance invitation.

### ExamAlert

To allow a user to remotely access a Windows 7 computer, you need to enable Remote Desktop or Remote Assistance through the firewall.

To enable Remote Assistance from the GUI, do the following:

1. Click **Start**, click **All Programs**, click **Maintenance**, and then click **Windows Remote Assistance**. This launches the Windows Remote Assistance screen, as shown in Figure 14.13. You can also click **Start** and type **assist** in the Start menu search box.
2. To get help, click **Invite someone you trust to help you**.
3. Select one of the following options:
  - ▶ **Save This Invitation to a File:** Selecting this option enables you to save your Remote Assistance invitation file to a folder. This folder can be a location on your computer or an available network Share.
  - ▶ **Use E-mail to Send an Invitation:** Selecting this option launches your default email client. A message is then created with an attached invitation file.
  - ▶ **Use Easy Connect:** Selecting this option creates and publishes your Remote Assistance invitation file using a 12-character password that you must communicate to whoever is helping you.

If you need to help someone, open Windows Remote Assistance and select **Help someone who has invited you**.

## Using Administrative Tools for Remote Hosts

Many of the Administrative Tools on a Windows 7 computer can be used to remotely manage a computer including those tools that are based on the Microsoft Management Console (MMC). To manage a computer using an MMC snap-in, follow these steps:

1. Log on to a remote computer.
2. Start an MMC snap-in, such as Computer Management, as shown in Figure 14.14.
3. In the left pane, right-click the top of the tree and click **Connect to another computer**. For example, in the Computer Management Console, you would right-click **Computer Management (Local)**.
4. In Another computer, type the computer name or IP address and click **OK**.

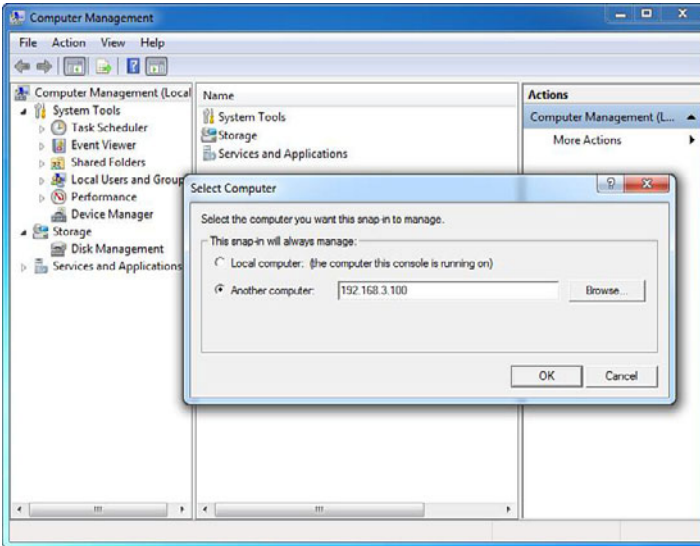


FIGURE 14.14 Connecting to another computer using MMC.

5. You can now use the MMC snap-in to manage the computer as you would any other computer running a Windows operating system.

You can also connect to a user's registry by opening the Registry Editor, opening the File menu, and selecting the **Connect Network Registry** option. For you to do this, the Remote Registry service must be running and you must have administrative permissions to the computer you want to connect to.

---

## Cram Quiz

1. What are the three ways that you can use to send an invitation to a user to connect using Remote Assistance? (Choose three answers.)
  - A. Save the invitation to a file
  - B. Use email to send an invitation
  - C. Use the Publish in Active Directory Invitation
  - D. Use Easy Connect



2. Which version of Windows 7 does NOT support Remote Desktop Hosting?
- A. Windows 7 Home Premium
  - B. Windows 7 Professional
  - C. Windows 7 Ultimate
  - D. Windows 7 Enterprise

## Cram Exam Answers

1. **A, B, and D** are correct. You can invite someone you trust by saving the invitation to file, using email to send an invitation, and using Easy Connect. You cannot send an invitation using Active Directory. Therefore, Answer C is incorrect because it is an option that does not exist.
  2. **A** is correct. You cannot use Remote Desktop Connection to connect to computers running Windows 7 Starter, Windows 7 Home Basic, Windows 7 Home Premium, and you can only create outgoing connections from those editions of Windows 7. Only Windows 7 Professional, Ultimate, and Enterprise editions support “Remote Desktop Hosting.”
-

# PowerShell

► **Configure remote management**

## CramSaver

1. What task-based command-line shell and scripting language is provided with Windows 7 that enables you to control local and remote computers and their Microsoft network services?
  - A. ActiveX
  - B. PowerShell
  - C. GPO
  - D. BackScript
2. What PowerShell command would you use to establish a connection with a remote computer running Windows 7?
  - A. Set-Location
  - B. EstablishPS
  - C. PSEstablishSession
  - D. New-PsSession

## Answers

1. **B** is correct. Windows PowerShell is a task-based command-line shell and scripting language to help IT professionals and users control and automate the administration of the Windows operating system and the applications that run on Windows. Answer A is incorrect because ActiveX is a control set used with web pages. Answer C is incorrect because GPO (short for Group Policy Object) is used to configure network environments. Answer D is incorrect because there is no such thing as BackScript.
2. **D** is correct. To establish a new session with a remote computer, you use the New-PsSession command. You can use PowerShell to execute commands remotely. Answer A is incorrect because the Set-Location command is used to change directories. Answers B and C are incorrect because these commands are invalid in PowerShell.

Windows PowerShell is a task-based command-line shell and scripting language to help IT professionals and users control and automate the administration of the Windows operating system and the applications that run on Windows. Windows PowerShell requires the Microsoft .NET Framework 2.0,

while the Windows PowerShell ISE requires the Microsoft .NET Framework 3.5 with Service Pack 1.

The Built-in Windows PowerShell commands are called cmdlets and enable you to manage client computers and servers, edit the registry and file system, perform WMI calls, and connect to the .NET Framework development environment. The Windows PowerShell commands can also be used to manage other Windows technologies, such as

- ▶ Active Directory Domain Services
- ▶ Windows BitLocker Drive Encryption
- ▶ DHCP Server service
- ▶ Group Policy
- ▶ Remote Desktop Services
- ▶ Windows Server Backup

Figure 14.15 shows the Windows PowerShell console.

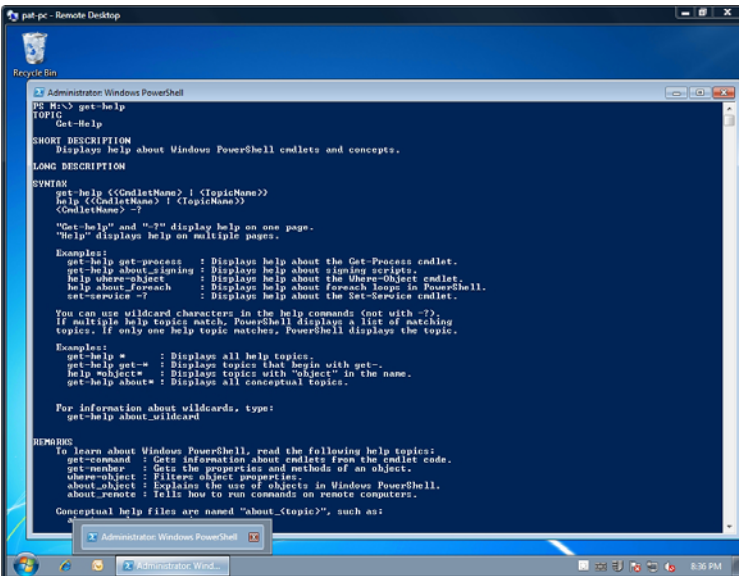


FIGURE 14.15 PowerShell console.

Although PowerShell was introduced with Windows Server 2007, the Windows PowerShell included with Windows 7 is PowerShell 2.0.

PowerShell 2.0 includes the following improvements of PowerShell 1.0:

- ▶ Hundreds of new cmdlets including `Get-Hotfix`, `Send-MailMessage`, `Get-ComputerRestorePoint`, `New-WebServiceProxy`, `Debug-Process`, `Add-Computer`, `Rename-Computer`, `Reset-ComputerMachinePassword`, and `Get-Random`.
- ▶ Remote management as commands can be run on one or multiple computers by establishing an interactive session from a single computer. Additionally, you can establish a session that receives remote commands from multiple computers.
- ▶ Windows PowerShell Integrated Scripting Environment (ISE), which is a graphical user interface where you can run commands and write, edit, run, test, and debug scripts in the same window. It includes a built-in debugger, multiline editing, selective execution, syntax colors, line and column numbers, and context-sensitive Help.
- ▶ Background jobs that run commands asynchronously and in the background while continuing to work in your session. You can run background jobs on a local or remote computer and store the results locally or remotely.
- ▶ The Windows PowerShell debugger helps debug functions and scripts. You can set and remove breakpoints, step through code, check the values of variables, and display a call-stack trace.
- ▶ Use Windows PowerShell modules to organize your Windows PowerShell scripts and functions into independent, self-contained units and package them to be distributed to other users. Modules can include audio files, images, Help files, and icons, and they run in a separate session to avoid name conflicts.
- ▶ The new event infrastructure helps you create events, subscribe to system and application events, and then listen, forward, and act on events synchronously and asynchronously.

Some popular PowerShell commands are as follows:

- ▶ **Clear-Host:** Clear the screen
- ▶ **Copy-Item:** Copy files or a directory
- ▶ **Get-ChildItem:** List all files or directories in the current directory

- ▶ **Get-Location:** Show the current directory
- ▶ **Move-Item:** Move a file or directory
- ▶ **Remove-Item:** Delete a file or directory
- ▶ **Rename-Item:** Rename a file or directory
- ▶ **Set-Location:** Change the current directory
- ▶ **Write-Output:** Print a string or variable onto the screen

One use for Windows 7 PowerShell is to execute a command on a target computer just as if you were sitting at the computer. To accomplish this, you perform these three steps:

1. Establish a session.
2. Execute any command, script, or cmdlet using the session.
3. Delete the session.

To establish a session, click the **Start** button, select **All Programs**, select **Accessories**, select **Windows PowerShell**, and select **Windows PowerShell**.

To create a session with a computer name called RemotePCName, use the following:

```
New-PsSession -ComputerName myremotepc
```

If you want to log in with a different username than you are currently logged in as, you execute the following command:

```
New-PsSession -ComputerName RemotePCName -credential $prompt
```

To run a command, such as the `ipconfig` command at a remote computer, perform the following commands:

```
$mysession = New-PSSession -ComputerName RemotePCName  
Invoke-Command { ipconfig } -Session $mysession
```

When you are done, it is always recommended to delete the session. To end the session, execute the following command:

```
Remove-PsSession -session $mysession
```

## Cram Quiz

1. What provides you a graphical user interface that enables you to run commands and write, edit, run, test, and debug scripts?
  - A. ISE
  - B. GPO
  - C. PSDebug
  - D. PS-Run
  
2. What PowerShell command is used to copy files?
  - A. Copy-Item
  - B. Set-Location
  - C. Write Output
  - D. Move-Item

## Cram Quiz Answers

1. **A** is correct. Windows PowerShell Integrated Scripting Environment (ISE) is a graphical user interface where you can run commands and write, edit, run, test, and debug scripts in the same window. Answer B is incorrect because GPO, short for Group Policy Object, enables you to configure network environments. Answers C and D are incorrect because the PSDebug or PS-Run programs don't exist.
  2. **A** is correct. To copy files or a directory using PowerShell, you use the Copy-Item command. Answer B is incorrect because the Set-Location command is used to change directories. Answer C is incorrect because the Write-Output command is used to print a string or variable onto the screen. Answer D is incorrect because the Move-Item command is used to move a file or directory.
-

## Review Questions

1. You work as the desktop support technician at Acme.com. You need to give a presentation using your mobile computer. So, you take the computer to the conference room and connect the projector to the computer with an S-Video cable. You want the desktop and Start menu to be displayed on the projector. What should you do in Windows 7?
  - A. Open Screen Resolution. Select the Projector from the Display options. Then select the Make this my main display option.
  - B. Open Personalization Settings. Select the icon that represents the laptop display. Then clear the Extend the desktop onto this monitor option.
  - C. Clear the Lock the taskbar option of the taskbar's context menu. Drag the taskbar as far to the right as possible.
  - D. Clear the Lock the taskbar option of the taskbar's context menu. Drag the taskbar as far to the left as possible.
2. You work as the desktop support technician at Acme.com. You have a laptop in a conference room connected to a large TV monitor. Because you forgot the power connector for the mobile computer, you want the battery to last as long as possible. What should you do to conserve the most power during the presentation?
  - A. Reduce the brightness settings in the Windows Mobility Center to the lowest setting
  - B. Select External display only in the New Display Detected dialog box
  - C. Select Extended in the New Display Detected dialog box
  - D. Turn on Presentation Mode in the Windows Mobility Center
3. You work as the desktop support specialist at Acme.com. You want to add a Bluetooth-enabled handheld device to your personal area networks (PAN). What do you need to do?
  - A. Configure the passkey and ensure that the device is discoverable
  - B. Configure the appropriate wireless security method and ensure that the device is discoverable
  - C. Turn on the Network Discovery and configure the passkey
  - D. Configure the passkey and ensure that the mobile device is Wi-Fi enabled

4. You work as the desktop support technician at Acme.com. You are planning to give a presentation on a tablet PC workstation. During the presentation, you need to temporarily block notifications and disable your screen saver. What should you do?
- A. You should set the screen saver to none in the Display Settings.
  - B. You should select Extended in the New Display Detected dialog box.
  - C. You should turn on and configure Presentation Mode in the Windows Mobility Center.
  - D. You should click Connect External Display in the Windows Mobility Center.
5. You work as the desktop support technician at Acme.com. You are in the office and get an emergency call to visit a client. You must be able to stop your work and resume as quickly as possible when you get to the client site. They also want to be protected from data loss if there is a power problem. What do you suggest?
- A. Ensure that the laptop workstations have Centrino hardware. You should configure hybrid sleep on the laptop workstations.
  - B. Ensure that the users are administrators. You should configure hybrid sleep on the laptop workstations.
  - C. Ensure that there is available disk space equivalent to the amount of RAM. Configure sleep on the laptop workstations.
  - D. Ensure that there is available disk space equivalent to the amount of RAM. You should configure hybrid sleep on the laptop workstations.
  - E. Ensure that there is available disk space equivalent to the amount of RAM. Configure hibernation on the laptop workstations.
6. You work as the desktop support technician at Acme.com. A user shuts down her PC by clicking the Power button icon on the Start menu; however, when she starts up her computer again, the same programs that were open when she tried to shut down are still open. What do you need to do so that her machine does a complete shutdown?
- A. Open Power Options, click the Choose what power buttons do link, and choose the option to shut the computer down when the power button is pressed.
  - B. Open Power Options, click the Change when computer sleeps link, and choose the option to never put the computer to sleep when it is running on battery.
  - C. Open Advanced Settings for the current power plan in Power Options. Change the Start menu power button setting to Shut down.
  - D. Change the On battery setting in the Sleep after category to Never.



7. You work as the desktop support technician at Acme.com. When you close the lid on your Windows 7 computer, you want to start working as soon as you restart the computer. You also don't want to use any battery power while the computer is shut down. What should you do?
- A. Configure the computer to hibernate when lid is closed
  - B. Configure the computer to sleep when lid is closed
  - C. Configure the computer to shut down when lid is closed
  - D. Configure the computer to go into standby when lid is closed
8. You work as the desktop support technician at Acme.com. You want to disable the Windows Media Player through the Windows SideShow. What should you do?
- A. Open the Windows SideShow and then turn off the Windows Media Player gadget
  - B. Open the Sync Center and remove the appropriate Sync partnership
  - C. Open the Windows Sidebar and turn off the Windows Media Player gadget
  - D. Open the Windows Media Player and then remove the appropriate plug-in
9. To use Windows Remote Desktop, a user must be added to one of two groups. What are the two groups? (Choose two.)
- A. Administrator
  - B. Power Users
  - C. Remote Desktop Administrators group
  - D. Remote Desktop Users group
10. What program is used to connect to a network project directly?
- A. Remote Desktop
  - B. Remote Assistance
  - C. Network Projector
  - D. Remote SideShow

# Review Question Answers

1. Answer **A** is correct. If you want to use the project as the main monitor, right-click the desktop and select Screen Resolution. Then select the Projector from the Display option and select Make this my main display. Answer B is incorrect because if you extend the desktop onto this monitor, the monitor and the project act together as if they were sitting side-by-side. Answers C and D are incorrect because the taskbar has nothing to do with the monitor configuration.
2. Answer **B** is correct. The LCD panel is one of the components on a laptop computer that uses the most power, so disabling the LCD panel conserves power. Therefore, you should select External display only in the New Display Detected dialog box. Answer A helps with power consumption but not as much as shutting off the LCD panel. Answers C and D do not reduce power consumption.
3. Answer **A** is correct. When you configure a Bluetooth-enabled handheld device, you need to enable Bluetooth and assign a passkey. Answers B, C, and D are incorrect because they are used to configure a wireless network connection, not Bluetooth.
4. Answer **C** is correct. When you turn on Presentation mode, your mobile PC stays awake and system notifications are turned off. You can also choose to turn off the screen saver, adjust the speaker volume, and change your desktop background image. Answer A is not the best answer because this only affects the screen saver and does not turn off system notifications and does not adjust speaker volume. Answers B and D affect only display settings.
5. Answer **C** is correct. When you perform hybrid sleep, it keeps the memory alive so that you can do a quick restart to where you left off. It also writes to the hard drive in case power is interrupted. Answer A is incorrect because you don't have to be an administrator. Answer B does not protect against power interruption. Answer D is incorrect because it is not the fastest to restart.
6. Answer **C** is correct. When the shutdown button is clicked, the system goes into either sleep mode or hibernate mode. Answer A is incorrect because you have to go into the Advanced options. Answer B is incorrect because you have to go into the Advanced options and there is not an option to never put to sleep mode. Answer D is incorrect because there is no such option.
7. Answer **A** is correct. You should configure the computer to hibernate when the lid is closed. Answer B is incorrect because hibernate is faster than setting the computer to sleep. Answer C is incorrect because shutdown is the slowest option from which to bring the computer back on. Answer D is incorrect because there is no standby mode in Windows 7.
8. Answer **A** is correct. Media Player can be accessed through SideShow. Therefore, you need to disable using the Control Panel. Answer B is incorrect because Sync is for data files, not Windows Media Player. Answer C is incorrect because, although both reference using gadgets, the Windows Media Player gadget is handled in the SideShow, not Sidebar. Answer D is not correct because the Windows Media Player is an application, not a plug-in.

9. Answers **A** and **D** are correct. All administrators are automatically given the necessary permission to use Windows Remote Desktop. For other users, you must add them to the Remote Desktop Users group. Answer B is incorrect because Power Users is mostly used for backward compatibility. Answer C is incorrect because there is no Remote Desktop Administrators group.
10. Answer **C** is correct. A network projector is a video projector that's connected to a wireless or wired local area network (LAN). What sets the network projector apart from other presentation methods is that you can connect to and operate the projector remotely over a network connection. If your computer can connect to the projector, you can deliver a presentation from any location that has network access, whether it's your private office or a conference room where the projector is located. Remote Desktop and Remote Assistance enables you to connect to a Windows computer. Answer D is incorrect because Windows SideShow uses gadgets, convenient mini programs, to extend information from your computer to other devices.

## CHAPTER 15

# Optimizing Windows 7 Systems

**This chapter covers the following 70-680 Objectives:**

- ▶ Monitoring and Maintaining Systems that Run Windows 7:
  - ▶ Monitor systems
  - ▶ Configure performance settings

Performance is the overall effectiveness of how data moves through the system. To be able to improve performance, you must determine the part of the system that is slowing down the throughput; it could be the speed of the processor, the amount of RAM on the machine, the speed of the disk system, the speed of the network adapter card, or some other factor. This limiting factor is referred to as the bottleneck of the system.

# Windows Performance Monitoring Tools

- ▶ Monitor systems
- ▶ Configure performance settings

## CramSaver

1. What tool gives you quick access to processor and memory utilization and which programs are using the processor and memory?
  - A. Task Manager
  - B. Performance Monitor
  - C. Windows Experience Index
  - D. Event Viewer
  
2. Which technology is used to improve performance of computers using a USB flash drive?
  - A. ReadyBoost
  - B. ReadyCache
  - C. ReadyDrive
  - D. ReadyUp
  
3. What measurement indicates that your processor is working too hard?
  - A. Consistently greater than 25%
  - B. Consistently greater than 50%
  - C. Consistently greater than 80%
  - D. Occasionally greater than 95%

## Answers

1. **A** is correct. A common tool used to quickly view system performance is the Windows Task Manager. Answer B is incorrect because the Performance Monitor provides a visual display of built-in Windows performance counters, either in real time or as a way to review historical data. Although the Performance Monitor is more powerful, it is not a quick-use tool. Answer C is incorrect because the Windows Experience Index measures the capability of your computer's hardware and software configuration and expresses this measurement as a number called a base score. Answer D is incorrect because the Event Viewer is used to view the Windows logs.

2. **A** is correct. Windows ReadyBoost boosts system performance by using USB flash devices as additional sources for caching. Answer C is incorrect because ReadyDrive boosts system performance on mobile computers equipped with hybrid drives. Answers B and D are incorrect because ReadyCache and ReadyUp do not exist in Windows 7.
3. **C** is correct. If the processor is at 80% all the time, you should upgrade the processor (using a faster processor, or adding additional processors) or move some the services or programs to other systems. Therefore, the other answers are incorrect.

Several tools that you can use to measure and monitor performance are as follows:

- ▶ Task Manager
- ▶ Windows Reliability and Performance Monitor
- ▶ Windows Experience Index

## Task Manager

A common tool used to quickly view system performance is the Windows Task Manager. As shown in Figure 15.1, the Performance tab includes four graphs. The top two graphs show how much CPU is being used at the moment and for the past few minutes. (If the CPU Usage History graph appears split, your computer either has multiple CPUs, a single dual-core CPU, or both.) A high percentage means that programs or processes are requiring a lot of CPU resources, which can slow your computer. If the percentage appears frozen at or near 100%, a program might not be responding.

The bottom two graphs display how much RAM, or physical memory, is being used in megabytes (MB), both at the current moment and for the past few minutes. The percentage of memory being used is listed at the bottom of the Task Manager window. If memory use seems consistently high or slows your computer's performance noticeably, try reducing the number of programs you have open at one time or installing more RAM.

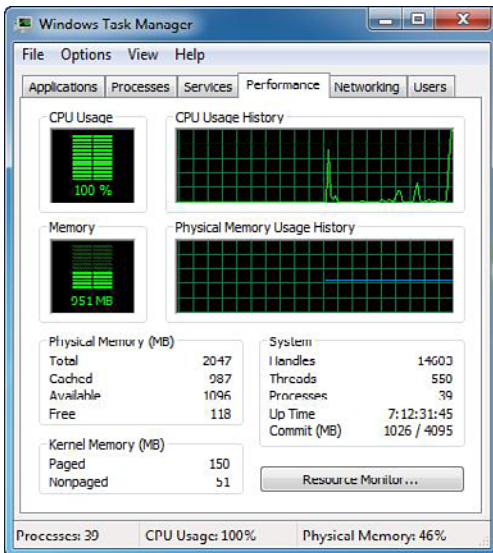


FIGURE 15.1 Window Task Manager showing the Performance tab.

To get a list of all individual processes or programs running in memory and how much processor utilization and memory usage each application is using, click the Processes tab to display the screen shown in Figure 15.2. You can also manually end any process here, which comes in handy when a process stops responding.

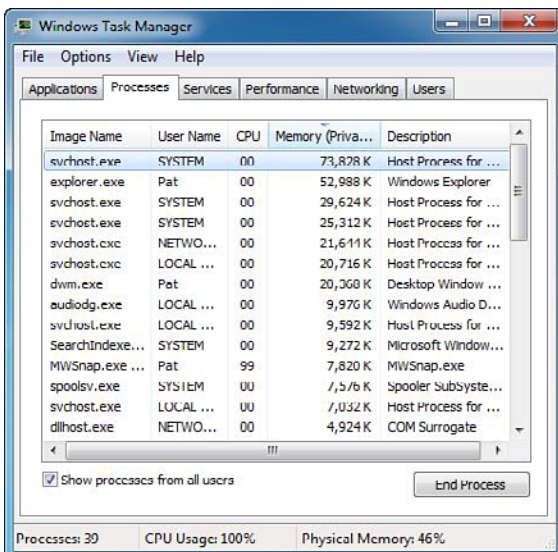


FIGURE 15.2 The Processes tab in Windows Task Manager.

**Note**

Sometimes when looking at Task Manager, you see an out-of-control process is the `svchosts.exe`, which is a generic service that can be utilized by multiple services. If you need to identify the specific application or service that is consuming too many resources, you might need to download and run Process Explorer, which you can find at <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>.

## Resource Monitor

Resource Monitor is a powerful tool that takes the Task Manager Processes tab one more step. Instead of just showing you the amount of processor and memory utilized for a process, it can also show you which applications are using files.

Windows Resource Monitor is a powerful tool for understanding how your system resources are used by processes and services. In addition to monitoring resource usage in real time, Resource Monitor can help you analyze unresponsive processes, identify which processes are accessing the disk, and which processes are utilizing the network.

To start Resource Monitor, click the **Start** button, click in the **Search programs and files** box, type `resmon.exe`, and then press **Enter**. You can also click the **Resource Monitor** button on the Performance tab within Task Manager.

Resource Monitor includes five tabs: Overview, CPU, Memory, Disk, and Network. The Overview tab displays basic system resource usage information; the other tabs display information about each specific resource.

By default, Resource Monitor displays real-time information about all of the processes running on your system. However, if you want to focus on a specific process or processes, you can filter data by doing the following:

1. Start **Resource Monitor** (see Figure 15.3).
2. Within any of the key tables, select the checkbox next to the name of each process you want to monitor in the Image column. Selected processes are moved to the top of the column.

To stop filtering for a single process or service, clear its checkbox. To stop filtering altogether, in the key table, clear the checkbox next to Image.



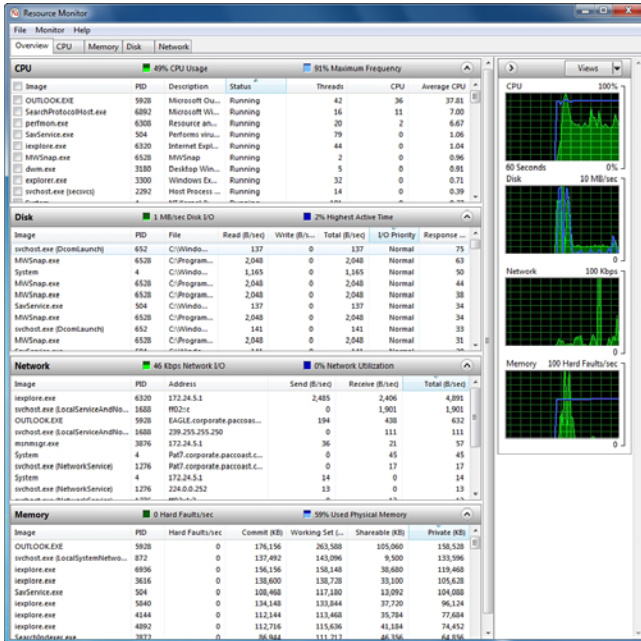


FIGURE 15.3 Resource Monitor.

## Performance Monitor

Performance Monitor provides a visual display of built-in Windows performance counters, either in real time or as a way to review historical data. You can add performance counters to Performance Monitor by dragging and dropping or by creating custom Data Collector Sets (DCS). Performance Monitor features multiple graph views that enable you to visually review performance log data. You can create custom views in Performance Monitor that can be exported as DCSs for use with performance and logging features. DCSs are explained shortly.

To be able to use Performance Monitor, the user must be an administrator or be a member of either the Performance Monitor Users group or the Performance Log Users group. Members of the Performance Monitor Users and Performance Log Users groups can view real-time performance data in Performance Monitor and can change the Performance Monitor display properties while viewing real-time data. The Performance Log Users group can also create or modify Data Collector Sets.

The four primary sub-systems that affect performance the most are processors, RAM, disk, and network performance. For example, the computer is centered around the processor. Therefore, the performance of the computer is greatly affected by the performance of the processor. The Processor:%Processor Time measures how busy the processor is. Although the processor might jump to 100% processor usage, the overall average is still important. If the processor is at 80% all the time, you should upgrade the processor (using a faster processor, or adding additional processors) or move some the services or programs to other systems.

**ExamAlert**

For the exam, be sure you know the multiple tools that can show you processor utilization, including the Task Manager and Performance Monitor. The processor utilization should not be consistently greater 80%.

RAM is another important factor in server performance. You can use the Performance Monitor to view how much available memory you have or how much paging is being done. *Paging* is when the disk space is used like RAM (virtual memory) so that it can allow Windows to load more programs and data. If the Performance Monitor shows no or little available memory or has a high pages/sec (20 or higher) or the paging file usage is high, you should increase the memory.

**ExamAlert**

Your pages/sec should not be 20 or higher and your paging file usage should not be greater than 1.5 times the RAM.

The Performance Monitor can also benefit you because if the server has a high processor utilization or high memory usage, you can determine which application is using most of the processor utilization or memory. Lastly, you can use Performance Monitor to set a baseline so that you know what is normal for the system. Then when you suspect poor performance, you can use the Performance Monitor to compare to the baseline so that you can quickly determine where the system is slowing down (bottleneck).

An important feature in Performance Monitor is the DCS, which groups data collectors into reusable elements. After a DCS is defined, you can schedule the collection of data using the DCS or see it in real time.

You can create a custom DCS containing performance counters and configure alert activities based on the performance counters exceeding or dropping below limits you define. After creating the DCS, you must configure the actions the system takes when the alert criteria are met.

### ExamAlert

A DCS can be used to define performance counters and how they are to be used, which can be saved and reused.

You can add performance counters to Performance Monitor by dragging and dropping or by creating custom DCSs. Performance Monitor features multiple graph views that enable you to visually review performance log data. You can create custom views in Performance Monitor that can be exported as DCSs for use with performance and logging features, as shown in Figure 15.4.

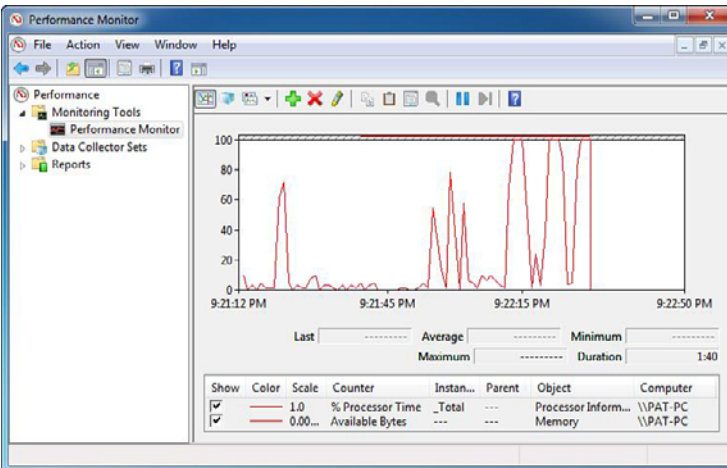


FIGURE 15.4 Performance Monitor.

## Windows Experience Index

The Windows Experience Index (WEI) measures the capability of your computer's hardware and software configuration and expresses this measurement as a number called a base score. A higher base score generally means that your computer performs better and faster than a computer with a lower base score, especially when performing more advanced and resource-intensive tasks.

To access the WEI, right-click **Computer** and select **Properties**. Then click **Windows Experience Index** to result in the screen shown in Figure 15.5.

If you recently upgraded your hardware, including changing drivers, and want to find out if your score has changed, click **Re-run the assessment**.

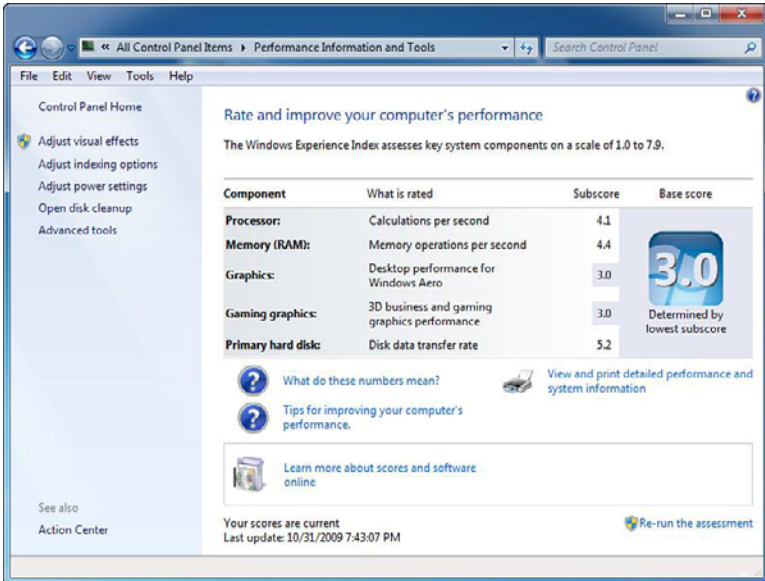


FIGURE 15.5 Windows Experience Index.

When looking at WEI, you see a base score, which is the lowest of all of the subscores. The subscores include processor, memory (RAM), graphics, gaming graphics, and primary hard disk. If you have processor, memory (RAM), graphics, and primary hard disk at 5.5 and the gaming graphics at 3.2, the base score is 3.2. Each score ranges from 1.0 to 7.9. Keep in mind that as hardware becomes faster, higher scores are achieved. When you purchase programs, keep in mind that some programs require a minimum WEI score.

The base score represents the minimum performance of your system based on the capabilities of different parts of your computer, including RAM, CPU, hard disk, general graphics performance on the desktop, and 3-D graphics capability.

Here are general descriptions of the experience you can expect from a computer that receives the following base scores:

- ▶ A computer with a base score of 1.0 or 2.0 usually has sufficient performance to do general computing tasks, such as run office productivity programs and search the Internet. However, a computer with this base score is generally not powerful enough to run Aero or the advanced multimedia experiences that are available with Windows 7.
- ▶ A computer with a base score of 3.0 can run Aero and many features of Windows 7 at a basic level. Some of the Windows 7 advanced features might not have all their functionality available. For example, a computer with a base score of 3.0 can display the Windows 7 theme at a resolution of 1280 × 1024 but might struggle to run the theme on multiple monitors. Or it can play digital TV content but might struggle to play high-definition television (HDTV) content.
- ▶ A computer with a base score of 4.0 or 5.0 can run new features of Windows 7, and it can support running multiple programs at the same time.
- ▶ A computer with a base score of 6.0 or 7.0 has a faster hard disk and can support high-end, graphics-intensive experiences, such as multiplayer and 3-D gaming and recording and playback of HDTV content.

## Memory Usage and the Paging File

When your computer does not have enough memory to perform all of its functions, Windows and your programs can stop working. To help prevent data loss, Windows notifies you when your computer is low on memory. Other signs of low memory include poor performance and screen problems. You can also check the Event Viewer and the Windows Reliability and Performance Monitor.

Your computer has two types of memory: random access memory (RAM), also known as physical memory, and virtual memory, also known as a paging file. All programs use RAM, but when there is not enough RAM for the program you're trying to run, Windows temporarily moves information that is normally stored in RAM to the virtual memory.

Virtual memory is disk space that acts like RAM, which enables the operating system to load more programs and data. Parts of all the programs and data to

be accessed are constantly swapped back and forth between RAM and disk so the virtual memory looks and acts like regular RAM. This is beneficial to the user because disk memory is far cheaper than RAM.

The RAM and virtual memory are broken down into chunks called pages, which are monitored by the operating system. When the RAM becomes full, the virtual memory system copies the least recently used programs and data to the virtual memory. Because this frees part of the RAM, it then has room to copy something else from virtual memory, load another program, or load more data. Windows 7 calls its virtual memory a paging file.

If you have low memory, you should consider the following:

- ▶ Installing more memory
- ▶ Increasing the size of the paging file
- ▶ Determining if a program overuses memory

To determine how much RAM you have, you can use the Welcome Center, Task Manager, or System Information. To open System Information:

1. Click the **Start** button and select **All Programs**.
2. Select **Accessories**, followed by selecting **System Tools**.
3. Select **System Information**.
4. The total amount of RAM is listed under total physical memory.

Windows 7 does a much better job in managing virtual memory than older versions of Windows. Windows 7 sets the minimum size of the paging file at the amount of RAM installed on your computer plus 300 MB and the maximum size at three times the amount of RAM installed on your computer. For most systems, if your paging file usage exceeds 1.5 times your RAM, your system experiences performance problems as it is paging to a slower disk more than it should.

If you want to manually manage virtual memory, you use a fixed virtual memory size in most cases. To do this, set the initial size and the maximum size to the same value. This ensures that the paging file is consistent and can be written to a single contiguous file (if possible, given the amount of space on the volume).

**ExamAlert**

A high value for pages/sec counter in performance monitor most likely means that you are low on physical memory because pages/sec shows how often it has to access the paging file.

Manually configure virtual memory by completing the following steps:

1. Click **Start** and then click **Control Panel**.
2. In Control Panel, click the **System and Security** category heading link.
3. Click **System**.
4. Click **Advanced System Settings** in the left pane.
5. Click **Settings** in the Performance section to display the Performance Options dialog box.
6. Click the **Advanced** tab and then click **Change** to display the Virtual Memory dialog box, as shown in Figure 15.6.
7. Clear the **Automatically manage paging file size for all drives** checkbox.
8. Under Drive [Volume Label], click the drive that contains the paging file you want to change.
9. Click **Custom size**, type a new size in megabytes in the Initial size (MB) or Maximum size (MB) box, click **Set**, and then click **OK**.

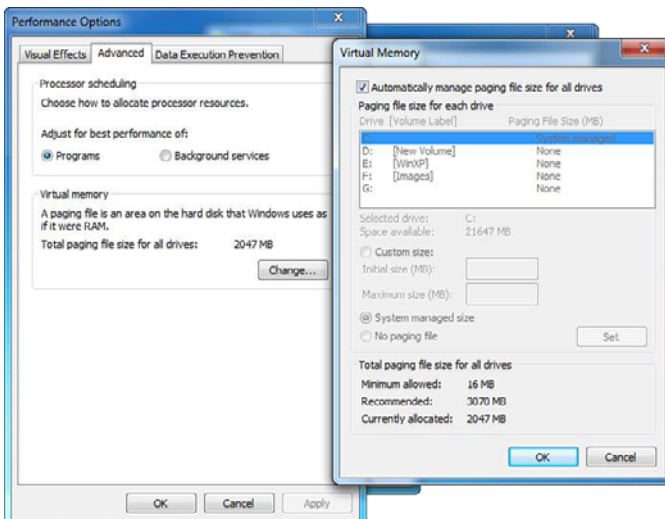


FIGURE 15.6 Modifying the Windows 7 paging file.

Increases in size usually do not require a restart, but if you decrease the size, you need to restart your computer for the changes to take effect. You should not disable or delete the paging file.

## Processor Scheduling

Computers running Windows 7 are usually used actively by users. Typically, these users want the programs that they are currently using to be given a higher priority than programs running in the background. However, if you have a Windows 7 workstation that is dedicated to a specific task, such as monitoring an assembly line or acting as a print server, you can have Windows share processor resources equally between background and foreground programs. To change the processor scheduling, you do the following:

1. Click the **Start** button, right-click **Computer**, and select **Properties**.
2. Click the **Advanced system settings**.
3. Click the **Advanced** tab.
4. Under Performance click **Settings**.
5. Click the **Advanced** tab.
6. Under Processor scheduling, choose one of the following:
  - ▶ Click **Programs** to assign more processor resources to the foreground programs.
  - ▶ Click **Background** services to assign equal amounts of processor resources to all running services.
7. Click **OK** to apply the changes and then click **OK** to close the System Properties dialog box.

## SuperFetch

SuperFetch is the caching technology used in Windows Vista and 7 that pre-loads commonly used applications into memory to reduce their load times. Besides caching recent applications (figuring that recent applications are more prone to be used again), it also keeps track of what time an application is being used so that it can load scheduled applications as necessary. To function more intelligently, SuperFetch can also ignore backups and virus scanners as normal caching technology that would also cache this information, although it is not necessary.



## ReadyBoost and ReadyDrive

Windows 7 has several features that affect how disks are used. These include the following:

- ▶ Windows ReadyBoost boosts system performance by using USB flash devices as additional sources for caching.
- ▶ Windows ReadyDrive boosts system performance on mobile computers equipped with hybrid drives.

With Windows ReadyBoost, USB flash devices with sufficiently fast memory (flash devices can be read up to 10 times faster than physical disk drives) are used to extend the disk caching capabilities of the computer's main memory. Using flash devices for caching enables Windows 7 to make random reads faster by caching data on the USB flash device instead of a disk drive. Because this caching is applied to all disk content, not just the page file or system dynamic-link libraries (DLLs), the computer's overall performance is boosted.

USB flash devices you can use with Windows ReadyBoost include USB 2.0 flash drives, Secure Digital (SD) cards, and CompactFlash cards. These devices must have sufficiently fast flash memory and be at least 256 MB or larger in size. Windows 7 can use up to eight devices totaling up to 256 GB.

When you insert a USB flash device into a USB 2.0 or higher port, Windows 7 analyzes the speed of the flash memory on the device. When you click **Speed Up My System Using Windows ReadyBoost**, Windows 7 extends the computer's physical memory to the device. The default configuration enables Windows ReadyBoost to reserve all available space on the device for boosting system speed.

To use Windows ReadyBoost with a USB flash device that you either already inserted or that you previously declined to use with Windows ReadyBoost, follow these steps:

1. Click **Start** and then click **Computer**.
2. Right-click the USB flash device in the **Devices with Removable Storage** list and then choose **Properties**.
3. On the **ReadyBoost** tab, select **Use This Device** and then click **OK**.
4. For USB flash devices that do not support ReadyBoost, you cannot enable the device. The only option you have is to stop retesting the device when you plug it in. The **Stop Retesting This Device When I Plug It In** option is selected by default.

If the USB flash drive has both slow and fast flash memory, you are not able to use the slow flash memory portion of the USB storage device to speed the computer performance. As a result, you might not see all of the memory of the USB device when it is added to your physical memory.

Windows ReadyDrive improves performance on mobile computers equipped with hybrid drives. A hybrid drive is a drive that uses both flash RAM and a physical drive for storage. Because flash RAM is much faster than a physical disk, mobile computers running Windows 7 write data and changes to data to the flash memory first and periodically sync these writes and changes to the physical disk. This approach reduces the spinning of the physical drive and thus saves battery power.

The flash RAM on hybrid drives can be used to provide faster startup and resume from sleep or hibernation. In this case, the information needed for starting or resuming the operating system is written to the flash RAM prior to shutting down, entering sleep, or going into hibernation. When you start or wake the computer, this information is read from the flash RAM.

You do not need to enable ReadyDrive as it is automatically enabled on mobile computers with hybrid drives.

---

## Cram Quiz

1. You have a computer running Windows 7. You need to frequently view performance data that encompasses processor usage, memory usage, disk usage, and network traffic over several days. What should you do?
  - A. Use the Task Manager
  - B. Add counters to the Performance Monitor
  - C. Use User Defined Data Collector Set
  - D. Use the Reliability Monitor
2. What measurement tool does Windows 7 offer to help determine if your system can run certain applications or perform certain functions of Windows 7?
  - A. WEI
  - B. CPUIndex
  - C. PagingGuide
  - D. PerfMon

3. How large does your USB drive have to be to make use of ReadyBoost?
- A. 256 MB
  - B. 512 MB
  - C. 1 GB
  - D. 2 GB

## Cram Quiz Answers

1. **C** is correct. An important feature in Performance Monitor is the Data Collector Set (DCS), which groups data collectors into reusable elements. After a Data Collector Set is defined, you can schedule the collection of data using the DCS or see it in real time. Answer A is incorrect because Task Manager only shows in real time and is not useful when you need to view overall performance over time. Answer B is incorrect because adding counters to the Performance Monitor only helps you view performance real time. Answer D is incorrect because the Reliability Monitor shows you potential problems with a system, not performance data.
  2. **A** is correct. The Windows Experience Index (WEI) measures the capability of your computer's hardware and software configuration and expresses this measurement as a number called a base score. A higher base score generally means that your computer performs better and faster than a computer with a lower base score, especially when performing more advanced and resource-intensive tasks. Answer D is incorrect because PerfMon is short for Performance Monitor, which is used to view performance indicators. It is mostly used to identify bottlenecks. It cannot determine if your system can run certain applications or perform certain functions. Answers B and C are incorrect because these terms do not exist in Windows 7.
  3. **A** is correct. USB flash devices that can be used with Windows ReadyBoost include USB 2.0 flash drives, Secure Digital (SD) cards, and CompactFlash cards. These devices must have sufficiently fast flash memory and be at least 256 MB or larger in size. Therefore, the other answers are incorrect.
-

# Review Questions

1. You work as the desktop support technician at Acme.com. You have a computer with 1 GB of memory running Windows 7 Ultimate. You want to add a fast removable flash drive to improve performance. What should you use?
  - A. Windows SuperFetch
  - B. Windows ReadyBoost
  - C. Windows ReadyDrive
  - D. Windows Memory Diagnostic tool
2. By default, what is the default configuration for processor scheduling on a computer running Windows 7?
  - A. Programs
  - B. Background
  - C. Balanced
  - D. Alternating
3. You insert a flash drive and discover that you cannot make use of all the memory on the USB flash device when configuring ReadyBoost. What do you think the problem is?
  - A. The USB flash drive has slow flash memory.
  - B. The USB flash drive has fast flash memory.
  - C. The USB flash drive has both slow and fast flash memory.
  - D. The USB flash drive does not meet the minimum requirement to configure ReadyBoost.
4. You work as the desktop support technician at Acme.com. You suspect an application is not releasing memory. You would like a user who is using the Windows 7 machine to run Performance Monitor. What do you need to do in order for the user to have access to Performance Monitor?
  - A. Add the user to the Power Users group
  - B. Add the user to the Performance Log Users group
  - C. Add the user to the Performance Monitor Users group
  - D. Add the user to the Administrator group

5. If you want to see if you are running out of physical memory, which counter should you use?
- A. CPU utilization
  - B. Pages\sec
  - C. Network utilization
  - D. interrupts\sec
6. What tool can help you quickly determine what processes are writing to disk and how much each is writing?
- A. System Information
  - B. System Configuration
  - C. Resource Monitor
  - D. Windows Experience Index
7. What should be the maximum memory page rate used for Windows 7?
- A. Less than 5
  - B. Less than 10
  - C. Less than 20
  - D. Less than 50
8. You have a system with 2 GB of memory. You notice that the processor utilization is around 65%, the paging file is around 4 GB, and the network traffic is around 5%. Your system seems sluggish. What do you think the problem is?
- A. Your processor is too slow.
  - B. You do not have enough memory.
  - C. Your network card is overtaxed.
  - D. Your disk system cannot keep up.
9. What can you use to quickly capture performance data of multiple performance counters and configure alert activities based on the performance counters?
- A. Alert Counter
  - B. Task Parameter
  - C. Data Collector Set
  - D. Windows Experience Index

10. What should the minimum WEI be if you want to support multiplayer or 3-D gaming and recording and playback of HDTV?
- A. 1.0
  - B. 2.0
  - C. 3.0
  - D. 4.0
  - E. 6.0

## Answers to Review Questions

1. Answer **B** is correct. Windows ReadyBoost boosts system performance by using USB flash devices as additional sources for caching. Answer A is incorrect because SuperFetch utilizes machine learning techniques to analyze usage patterns in order to enable Windows 7 to make intelligent decisions about what content should be present in system memory at any given time. Answer C is incorrect because ReadyDrive boosts system performance on mobile computers equipped with hybrid drives. Answer D is incorrect because the Windows Memory Diagnostic tool is used to test memory and not to increase performance.
2. Answer **A** is correct. By default, processor scheduling is set to Programs, which assigns more processor resources to the foreground programs. Answer B is incorrect because when Background services is selected, equal amounts of processor resources go to all running services. Answers C and D are incorrect because Balanced and Alternating do not exist in processor scheduling.
3. Answer **C** is correct. To get the benefit of ReadyBoost, your USB device needs to use fast flash memory. Therefore, if you insert a USB flash device that consists of slow and fast flash memory, ReadyBoost only uses the fast flash memory. Answers A and B are incorrect. Because ReadyBoost recognizes some of the memory, you can assume that the USB flash device meets the minimum requirements, so Answer D is incorrect.
4. Answers **B** and **C** are correct. For standard users to run the performance monitor, you must add them to the Performance Monitor Users group or Performance Log Users group, or you can make them administrators. Because there is no need to make them administrators, it is best to add them only to the Performance Monitor group or the Performance Log Users group. The difference between the two groups is that the Performance Log Users group can also create and modify Data Collector Sets but the Performance Monitor group cannot. Therefore, Answer D is incorrect. Answer A is incorrect because Power Users groups are only there for backward compatibility for older applications created for older versions of Windows.

5. Answer **B** is correct. To see how much paging takes place between physical RAM and the paging file (disk space acting as RAM), you refer to the pages\sec measurement. A high value indicates that you are utilizing the paging often, which means you are running out of physical memory. Answer A is incorrect because CPU utilization shows how hard the processor is working. Answer C is incorrect because network utilization indicates how much bandwidth is being used on the network. Answer D is incorrect because a high value for Interrupts\sec might indicate a faulty device or device driver.
6. Answer **C** is correct. Resource Monitor shows you the amount of processor and memory utilized for a process in addition to indicating which applications are using files. Windows Resource Monitor is a powerful tool for understanding how your system resources are used by processes and services. Answer A is incorrect because System Information shows the hardware and software running on a computer. Answer B is incorrect because the System Configuration is a troubleshooting tool to help you isolate problematic startup programs. Answer D is incorrect because the Windows Experience Index is used to gauge the performance of a system.
7. Answer **C** is correct. If the Performance Monitor shows no or little available memory or has a high pages/sec (20 or higher) or the paging file usage is high, you should increase the memory. Therefore, the other answers are incorrect.
8. Answer **B** is incorrect. Most likely your paging file is too large, which causes excessive paging because the paging file (disk) is much slower than RAM. Therefore, you should add more memory. Answer A is incorrect because if the processor was too busy, it would consistently be greater than 80%. Answer C is incorrect because the network traffic is low. Answer D is incorrect because the paging file has grown beyond 1.5 times memory. If you have a bottleneck for disk, you have to look at additional performance counters such as the length of the disk queue.
9. Answer **C** is correct. An important feature in Performance Monitor is the Data Collector Set (DCS), which groups data collectors into reusable elements. After a DCS is defined, you can schedule the collection of data using the DCS or see it in real time. Answer D is incorrect because the Windows Experience Index measures the capability of your computer's hardware and software configuration and expresses this measurement as a number called a base score. Answers A and B are incorrect because alert counter and task parameters are not part of performance monitoring or do not exist.
10. Answer **E** is correct. A computer with a base score of 6.0 or 7.0 has a faster hard disk and can support high-end, graphics-intensive experiences, such as multiplayer and 3-D gaming and recording and playback of HDTV content. Therefore, the other answers are incorrect.

## CHAPTER 16

# Backups and System Recovery

### **This chapter covers the following 70-680 Objectives:**

- ▶ Monitoring and Maintaining Systems That Run Windows 7:
  - ▶ Monitor systems
- ▶ Configuring Backup and Recovery Options:
  - ▶ Configure backup
  - ▶ Configure file recovery options
  - ▶ Configure system recovery options

Reliability is the ability of a computer to perform and maintain its functions in routine circumstances. When problems (application crashes, service freezes and restarts, driver initialization failures, and operating system failures) occur, reliability is affected because the computer cannot perform and maintain its functions.

Windows 7 architecture has the capability to detect and correct some problems. Windows 7 also provides multiple diagnostic programs to guide you through troubleshooting a wide range of problems. Of course, with the more complicated problems, you need to use basic troubleshooting methodology while using the wide range of troubleshooting tools available. Don't forget that performing backups on a regularly basis is invaluable when all else fails.



# Looking at Events

- ▶ Monitor systems
- ▶ Configure system recovery options

## CramSaver

1. In Windows 7, what can be used to quickly view if your antivirus is up to date and if Windows is patched?
  - A. Event Viewer
  - B. Action Center
  - C. Reliability Monitor
  - D. System Information
  
2. What key do you need to press to enter Safe mode?
  - A. F1
  - B. F4
  - C. F8
  - D. F10
  
3. What tool do you use to disable several programs that automatically start up during boot up?
  - A. System Configuration
  - B. System Information
  - C. Action Center
  - D. BCDBoot

## Answers

1. **B** is correct. Action Center is a central place to view alerts and take actions that can help keep Windows running smoothly. Action Center notifies you when items need your attention and lists important messages about security and maintenance settings that need your attention. Answer A is incorrect because the Event Viewer enables you to look at the Windows logs. Answer C is incorrect because the Reliability Monitor gives you an overview of the system stability and enables you to view individual events that effect overall stability. Answer D is incorrect because the System Information gives you an overview of the system, including the recognized hardware and software.

2. **C** is correct. By pressing the F8 key, you can enter the Advanced Startup menu and select Safe Mode. Answer A is incorrect because the F1 key is usually used for help. It could also be used to access the ROM BIOS program on some computers. Answer B is incorrect because the F4 key was used to load disk drivers during the installation of Windows XP, not Windows 7. Answer D is incorrect because the F10 key can be used to access the ROM BIOS program on some computers.
3. **A** is correct. System Configuration is an advanced tool that can help identify problems that might prevent Windows from starting correctly. You can start Windows with common services and startup programs turned off and then turn them back on, one at a time. Answer B is incorrect because the System Information is used to view a system's configuration. Answer C is incorrect because the Action Center is a central place to view alerts and take actions that can help keep Windows running smoothly. Answer D is incorrect because the BCDBoot is used to configure which operating system to boot if you have more than one copy of Windows installed.

When trying to troubleshoot problems, you usually need to gather as much information as possible to provide insight on the actual problem or help you to identify potential problems. Windows 7 has several tools to help you take a look at the system and its health.

## Event Viewer

Event Viewer, as shown in Figure 16.1, is a utility that is used to view and manage logs of system, application, and security events on a computer. Event Viewer gathers information about hardware and software problems and monitors Windows security events. Event Viewer can be executed by opening Administrative Tools and clicking **Event Viewer**, or by adding it to the Microsoft Management Console (MMC). It is also part of the Computer Management Console. You can also open it by executing `eventvwr.msc` at a command prompt or using the **Run** option.

### ExamAlert

Most Windows and application errors are displayed in the Event Viewer, which you can access by itself or as part of the Computer Management Console.

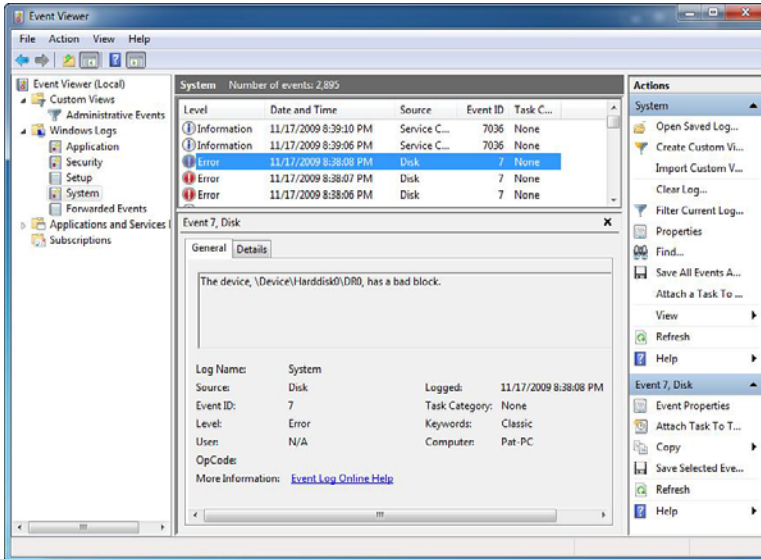


FIGURE 16.1 Event Viewer.

The newer version of Event Viewer available with Windows 7 is divided into Custom Views, Windows Logs, Applications and Services, and Subscriptions. Traditional logs that have been included with Windows XP and Windows Vista are found in the Windows Logs group. They include the following:

- ▶ **Application:** The application log contains events logged by programs. For example, a database program might record a file error in the programs log. Program developers decide which events to monitor. The application log can be viewed by all users.
- ▶ **Security:** The security logs contains valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files or other objects. For example, if you have enabled logon and logoff auditing, attempts to log on to the system are recorded in the security log. By default, security logging is turned off. To enable security logging, use Group Policies to set the audit policy or change the registry. To audit files and folders, you must be logged on as a member of the Administrators group or have been granted the Manage auditing and security log right in Group Policies. Security logs can only be viewed by administrators.

- ▶ **System:** The system log contains events that are logged by the Windows system components. For example, the failure of a driver or other system component to load during start-up is recorded in the system log. The event types logged by system components are predetermined by Windows. The system log can be viewed by all users.

There are five levels of events:

- ▶ **Error:** A significant problem occurs, such as loss of data or loss of functionality (for example, when a service fails during start-up).
- ▶ **Warning:** An event that is not necessarily significant, but might indicate a possible future problem. For example, when disk space is low, a warning is logged.
- ▶ **Information:** An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an information event is logged.
- ▶ **Success Audit:** An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system is logged as a success audit event.
- ▶ **Failure Audit:** An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a failure audit event.

When you double-click an event, the Event Properties window appears. The Event Properties can be divided into two parts, event header and event description. The event header information includes:

- ▶ **Date:** The date the event occurred.
- ▶ **Time:** Local time the event occurred.
- ▶ **User:** User name on whose behalf the event occurred.
- ▶ **Computer:** Name of the computer where the event occurred. The computer name is usually the local computer unless you are viewing an event log on another Windows computer.
- ▶ **Event ID:** Number identifying the particular event type.
- ▶ **Source:** Software that logged the event, which can be either a program name, such as SQL Server, or a component of the system or of a large program, such as a driver name.

- ▶ **Type:** Classification of the event severity: error, information, or warning in the system and application logs; and success audit and failure audit in the security log.
- ▶ **Category:** Classification of the event by the event source.

## Filtering Events

When you go through an Event Viewer, you see that some of these logs have hundreds, even thousands, of entries. When you are looking for something specific, it can be a daunting task to find it. To help you cut down on the log entries to review, the Event Viewer enables you to filter the current logs by opening the Action menu and selecting Filter Current Log, as shown in Figure 16.2. From here, you can specify the event level, ID, keywords, users, and/or computers.

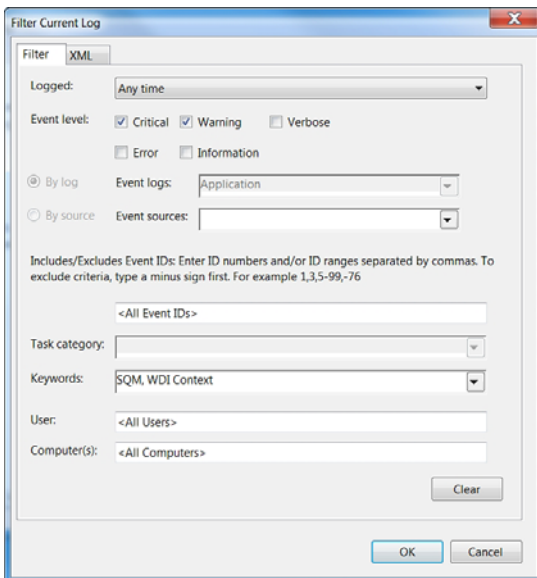


FIGURE 16.2 Filtering the Event Viewer logs.

## Event Subscriptions

If you need to review the events of multiple computers, you have to log on to each computer to access the Event Viewer or open multiple event viewer views, one for each computer that you need to review. Starting with Windows Vista, Windows has the capability to collect copies of events from multiple

remote computers and store them locally. To specify which events to collect, you create an event subscription.

To configure computers in a domain to forward and collect events:

1. Log on to each source computer with an account that has administrative privileges.
2. Execute the following command:
 

```
winrm quickconfig
```
3. Add the computer account to which you want the logs to be sent to the local Administrators group.
4. On the collector computer, execute the following command:
 

```
wecutil qc
```

The events appear in the Forwarded Events logs.

## Reliability Monitor

Besides combing through the Event Viewer, you can use the Reliability Monitor to give you an overview of the system stability and to view individual events that effect overall stability, as shown in Figure 16.3. Some of the events shown are software installation, operating system updates, and hardware failures.

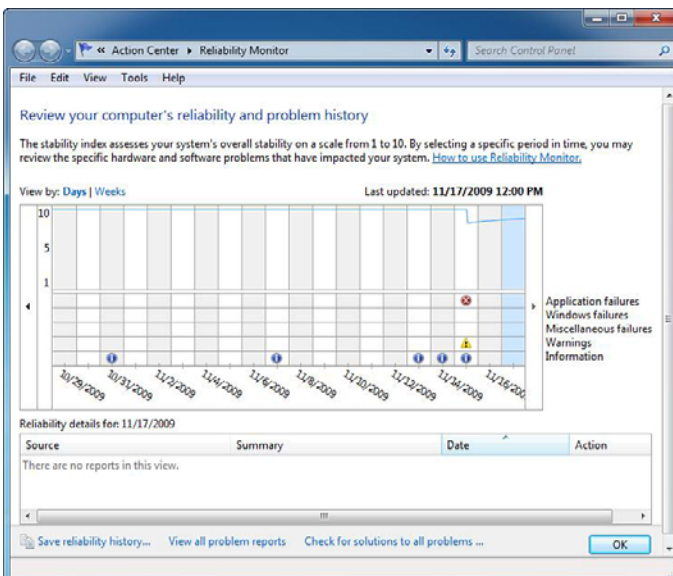


FIGURE 16.3 Reliability Monitor.

Reliability Monitor calculates a System Stability Index that reflects whether unexpected problems reduced the reliability of the system. A graph of the Stability Index over time quickly identifies dates when problems began to occur. The accompanying System Stability Report provides details to help troubleshoot the root cause of reduced reliability. By viewing changes to the system (installation or removal of applications, updates to the operating system, or addition or modification of drivers) side-by-side with failures (application failures, operating system crashes, or hardware failures), you can quickly develop a strategy for addressing the issues.

## Action Center

Action Center is a central place to view alerts and take actions that can help keep Windows running smoothly, as illustrated in Figure 16.4. Action Center notifies you when items need your attention and lists important messages about security and maintenance settings that need your attention. Red items in Action Center are labeled Important and indicate significant issues that should be addressed soon, such as an outdated antivirus program that needs updating. Yellow items are suggested tasks that you should consider addressing, such as recommended maintenance tasks.

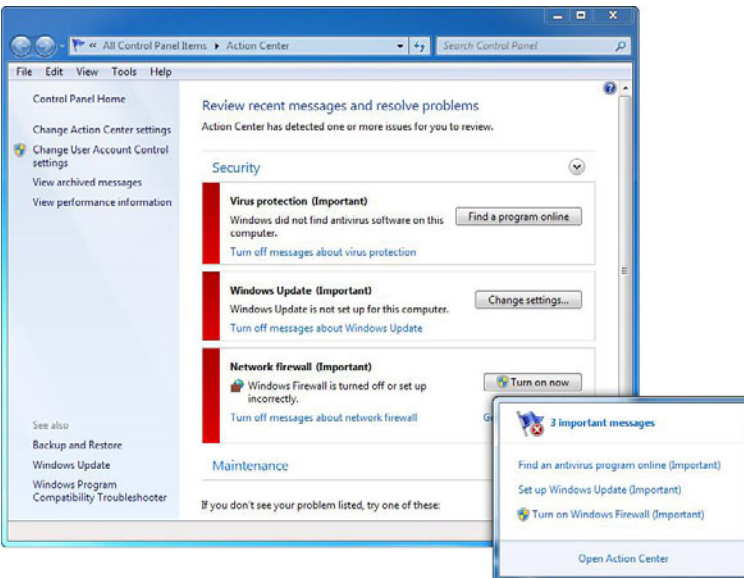


FIGURE 16.4 Action Center.

To view details about either the Security or Maintenance section, click the heading or the arrow next to the heading to expand or collapse the section. If you don't want to see certain types of messages, you can choose to hide them from view.

You can quickly see whether there are any new messages in Action Center by placing your mouse over the Action Center icon in the notification area on the taskbar. Click the icon to view more detail, and click a message to address the issue. Or open Action Center to view the message in its entirety.

## System Information

System Information (also known as msinfo32.exe) shows details about your computer's hardware configuration, computer components, and software, including drivers, as shown in Figure 16.5. Microsoft created System Information so that support personnel can quickly identify the Windows configuration.

System Information lists categories in the left pane and details about each category in the right pane. The categories include the following:

- ▶ **System Summary:** Displays general information about your computer and the operating system, such as the computer name and manufacturer, the type of basic input/output system (BIOS) your computer uses, and the amount of memory that's installed
- ▶ **Hardware Resources:** Displays advanced details about your computer's hardware and is intended for IT professionals
- ▶ **Components:** Displays information about disk drives, sound devices, modems, and other components installed on your computer
- ▶ **Software Environment:** Displays information about drivers, network connections, and other program-related details

To find a specific detail in System Information, type the information you're looking for in the **Find what** box at the bottom of the window. For example, to find your computer's Internet protocol (IP) address, type **ip address** in the Find what box and then click **Find**.



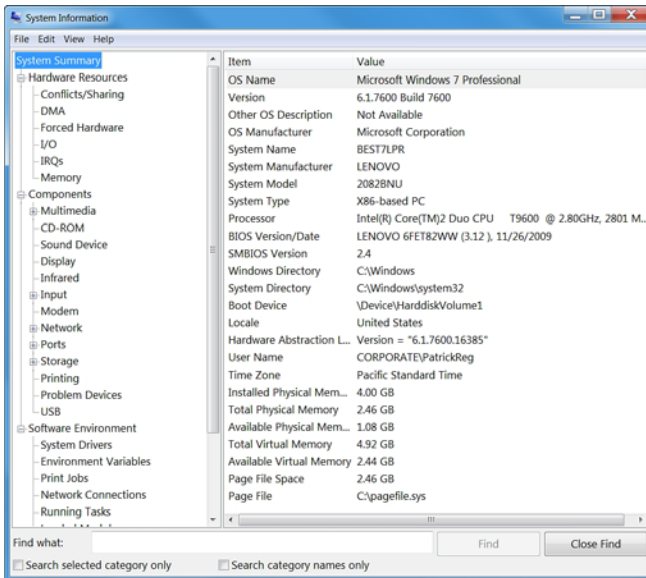


FIGURE 16.5 System Information.

## Diagnostic Tools

Windows 7 has multiple tools for diagnosing and resolving problems. To proactively and automatically identify potential problems, Windows 7 includes built-in diagnostics that can automatically detect and diagnose common support problems. The Windows 7 built-in diagnostics can automatically identify and help users resolve the following problems:

- ▶ Hardware error conditions
- ▶ Failing disks
- ▶ Degraded performance
- ▶ Failure to shut down properly
- ▶ Memory problems
- ▶ Problems related to installing drivers and applications
- ▶ Problems related to using drivers and applications

In most cases, the built-in diagnostics prompt users to make them aware of any problems as they occur and then help to guide users through resolving the problem.

## Memory Diagnostic Tool

Bad memory can cause a wide assortment of problems with your system including causing Windows not to be reliable. The Memory Diagnostic tool is used to diagnose physical memory problems, including memory leaks and failing memory. The tool also works with the Microsoft Online Crash Analysis tool to detect system crashes possibly caused by failing memory, which then prompts the user to schedule a memory test the next time the computer is restarted.

If you suspect that a computer has a memory problem that is not being automatically detected, you can run Windows Memory Diagnostics manually by completing the following steps:

1. Click **Start**, point to **All Programs**, and then click **Accessories**.
2. Right-click **Command Prompt** and then select **Run As Administrator**.
3. At the command prompt, type `mdsched.exe`.
4. You can choose to restart the computer and run the tool immediately or schedule the tool to run at the next restart.

You can also manually run the Windows Memory Diagnostics tool from Administrative Tools in Control Panel or from the boot menu before Windows loads.

If you choose to run the tool at the next restart, Windows Memory Diagnostics runs automatically after the computer restarts, enabling you to choose the type of testing to perform. When the computer restarts and the memory is tested, you are provided with an easy-to-understand report detailing the problem. Information is also written to the event log for future analysis.

While the test is running, you can press **F1** to access advanced diagnostic options. The advanced options include the following:

- ▶ **Test mix:** Choose what type of test you want to run
- ▶ **Cache:** Choose the cache setting you want for each test
- ▶ **Pass Count:** Type the number of times you want to repeat the tests

Press the **Tab** key to move between the different advanced options. When you have selected your options, press **F10** to start the test.

## Network Diagnostic Tool

The Windows Network Diagnostic tool was discussed in Chapter 5, “Configuring Windows Networking,” to help resolve network-related issues. When a user is unable to connect to a network resource, the user is presented with a repair option, which runs the Windows Network Diagnostic tool. You can also choose to run the tool manually by using the Diagnose option on the Local Area Connections Status property sheet.

## Boot Tools

When dealing with Windows, you eventually deal with boot problems. Either the computer does not boot completely or you get errors during boot up. Windows 7 offers several tools in troubleshooting these types of problems, as described in the sections that follow.

## Advanced Startup Options

The Advanced Boot Options menu lets you start Windows in advanced troubleshooting modes. To access the advanced startup options, do the following:

- ▶ If your computer has a single operating system installed, repeatedly press the **F8** key as your computer restarts. You need to press **F8** before the Windows logo appears. If the Windows logo appears, you need to try again.
- ▶ If your computer has more than one operating system, use the arrow keys to highlight the operating system you want to start in Safe Mode and then press **F8**.

On the Advanced Boot Options screen shown in Figure 16.6, use the arrow keys to highlight the Safe Mode option you want and then press **Enter**. Log on to your computer with a user account that has administrator rights. When your computer is in Safe Mode, you see the words *Safe Mode* in the corners of the display. To exit Safe Mode, restart your computer and let Windows start normally.

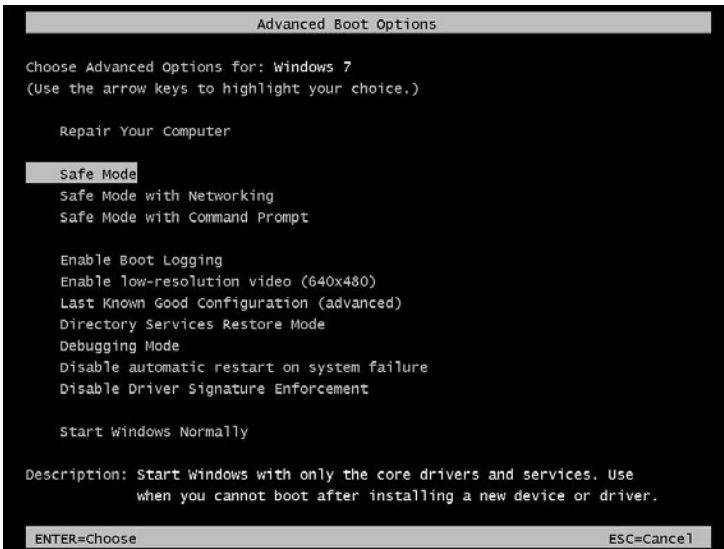


FIGURE 16.6 Advanced Boot Options.

Some options, such as Safe Mode, start Windows in a limited state, where only the bare essentials are started. If a problem does not reappear when you start in Safe Mode, you can eliminate the default settings and basic device drivers as possible causes. Other options start Windows with advanced features intended for use by system administrators and IT professionals.

The available options are as follows:

- ▶ **Repair Your Computer:** Shows a list of system recovery tools (Startup Repair Tool) you can use to repair startup problems, run diagnostics, or restore your system. This option is available only if you install the tools onto the computer. If they are not installed, the system recovery tools are located on the Windows installation disc.
- ▶ **Safe Mode:** Starts Windows with a minimal set of drivers and services. While in Safe Mode, shown in Figure 16.7, you can access the Control Panel, Device Manager, Event Viewer, System Information, Command Prompt, and Registry Editor.
- ▶ **Safe Mode with Networking:** Starts Windows in Safe Mode but also enables networking.
- ▶ **Safe Mode with Command Prompt:** Starts Windows in Safe Mode with a command prompt window instead of the Windows graphical user interface (GUI). This option is intended for IT professionals and administrators.

- ▶ **Enable Boot Logging:** Lists all of the drivers that are installed during startup in the `ntbtlog.txt` file. The `ntbtlog.txt` file can be used to determine which driver failed if Windows cannot start properly.
- ▶ **Enable low-resolution video (640 × 480):** Boots to the Windows GUI in minimal VGA mode using the standard VGA drivers (640 × 480 resolution and 16 colors).
- ▶ **Last Known Good Configuration (advanced):** Starts Windows with the last registry and driver configuration that worked when the last user logged on successfully.
- ▶ **Directory Services Restore Mode:** Starts Windows in Directory Services Restore Mode so that you can restore or repair Active Directory.
- ▶ **Debugging Mode:** Shows driver names as the drivers are loaded during the boot process.
- ▶ **Disable automatic restart on system failure:** Prevents Windows from automatically restarting if an error occurs during bootup. Use this option if Windows constantly fails and reboots.
- ▶ **Disable Driver Signature Enforcement:** Allows drivers containing improper signatures to be installed.
- ▶ **Start Windows normally:** Starts Windows in its normal mode.

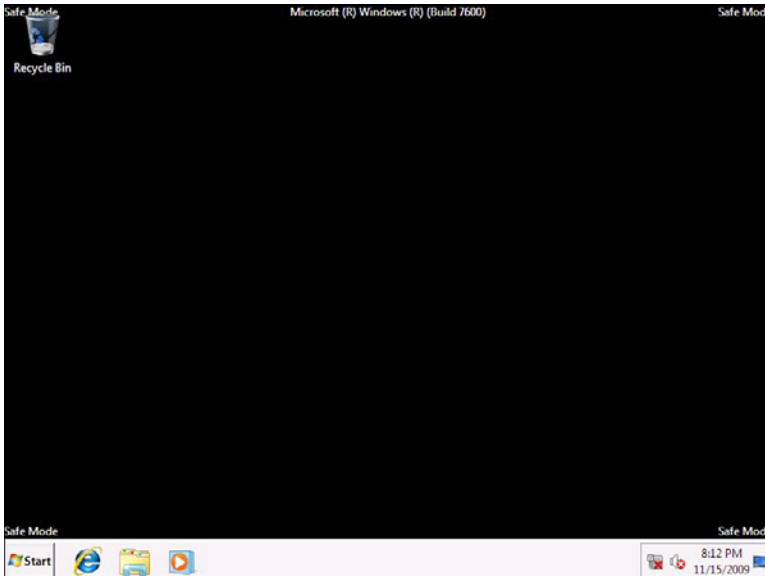


FIGURE 16.7 Safe Mode.

## System Configuration

System Configuration is an advanced tool that can help identify problems that might prevent Windows from starting correctly. You can start Windows with common services and startup programs turned off and then turn them back on, one at a time. If a problem does not occur when a service is turned off but does occur when turned on, then the service could be the cause of the problem. System Configuration is intended to find and isolate problems, but it is not meant as a startup management program.

The System Configuration tool can be loaded from the Administrative Tools. The tabs found in System Configuration tool are shown in Table 16.1.

TABLE 16.1 **System Configuration Tool Tabs**

Tab	Description
General	<p>Lists choices for startup configuration modes:</p> <p><b>Normal startup:</b> Starts Windows in its normal mode.</p> <p><b>Diagnostic startup:</b> Starts Windows with basic services and drivers only. If Diagnostic startup starts without a problem, it verifies that the problem is not the basic Windows files.</p> <p><b>Selective startup:</b> Starts Windows with basic services and drivers and enables you to select individual services and startup programs. Select startup is used to isolate problematic services and startup programs.</p>
Boot	<p>Shows configuration options for the operating system and advanced debugging settings, including:</p> <p><b>Safe boot-Minimal:</b> Boots Windows into Safe Mode with GUI interface, which runs only essential system services. Networking is disabled.</p> <p><b>Safe boot-Alternate shell:</b> Boots to the Safe Mode (command prompt). Networking and the graphical user interface are disabled.</p> <p><b>Safe boot-Active Directory repair:</b> Starts Windows in Directory Services Restore Mode so that you can restore or repair Active Directory.</p> <p><b>Safe boot-Network:</b> Boots Windows into Safe Mode, which runs only essential system services but also enables networking.</p> <p><b>Boot log:</b> Lists all of the drivers that are installed during startup in the ntbtlog.txt file. The ntbtlog.txt file can be used to determine which driver failed if Windows cannot start properly.</p> <p><b>Base video:</b> Boots to the Windows graphical user interface in minimal VGA mode using the standard VGA drivers (640 × 480 resolution and 16 colors).</p> <p><b>OS boot information:</b> Shows driver names as the drivers are loaded during the boot process.</p> <p><b>Make all settings permanent:</b> Does not track changes made in System Configuration. Options can be changed later using System Configuration, but must be changed manually. When this option is selected, you cannot roll back your changes by selecting Normal startup on the General tab.</p>

TABLE 16.1 **Continued**

Tab	Description
Services	Lists all services that are registered with Windows and displays their current status (running or stopped). You can use the Services tab to enable or disable individual services so that you can isolate a problematic service that loads during boot up.  You can select Hide all Microsoft services to show only third-party applications in the services list.
Startup	Lists applications that start when the computer boots, including the name of their publishers, the paths to the executable files, and the locations of the registry keys or shortcuts that cause the applications to run, as shown in Figure 16.8. This option is used to isolate problematic programs that load during boot up.
Tools	Provides a list of diagnostic tools, as shown in Figure 16.9.

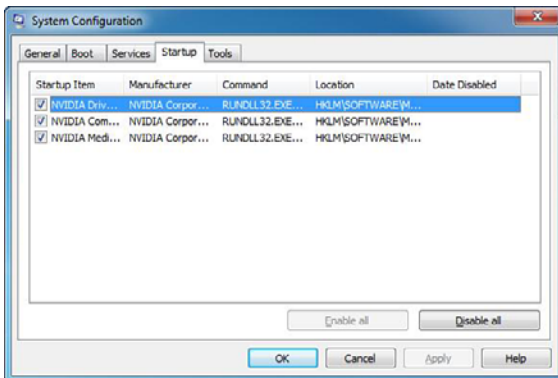


FIGURE 16.8 System Configuration Startup tab.

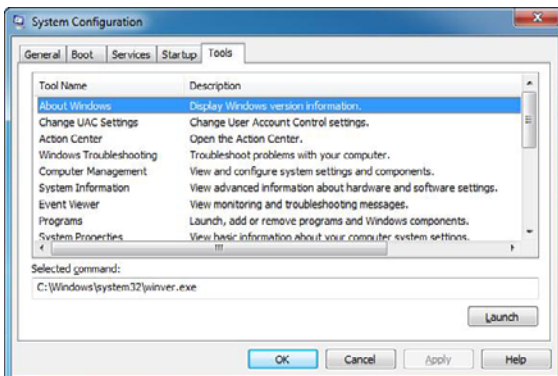


FIGURE 16.9 System Configuration Tools tab.

A new component that has been added to Windows 7 System Configuration is the ability to increase Windows 7 boot speed. If you select the Boot options and click the **Advanced Options**, you can increase the number of processors used during boot up, assuming you have multiple processors. As a result, you have a quicker boot time.

## System Recovery Disc

The System Recovery Options menu contains several tools, such as Startup Repair, that can help you recover Windows from a serious error. This set of tools is on your computer's hard disk and on the Windows installation disc.

To open the System Recovery Options menu on your computer, do the following:

1. Remove all floppy disks, CDs, and DVDs from your computer and then restart your computer using the computer's power button.
2. Do one of the following:
  - ▶ If your computer has a single operating system installed, press and hold the **F8** key as your computer restarts. You need to press **F8** before the Windows logo appears. If the Windows logo appears, you need to try again by waiting until the Windows logon prompt appears and then shutting down and restarting your computer.
  - ▶ If your computer has more than one operating system, use the arrow keys to highlight the operating system you want to repair and then press and hold **F8**.
3. On the Advanced Boot Options screen, use the arrow keys to highlight Repair your computer and then press **Enter**. (If Repair your computer isn't listed as an option, your computer doesn't include preinstalled recovery options, or your network administrator has turned them off.)
4. Select a keyboard layout and then click **Next**.
5. On the System Recovery Options menu, click a tool to open it, as shown in Figure 16.10.



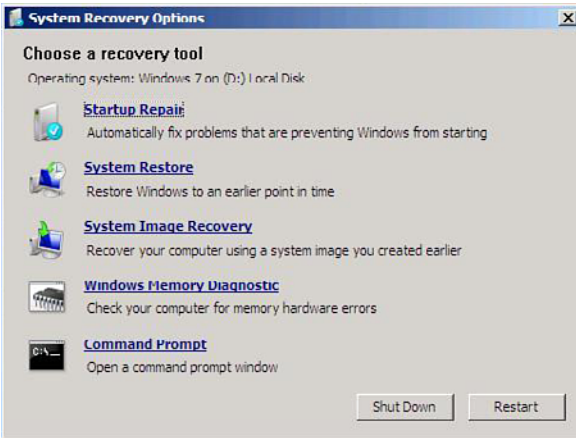


FIGURE 16.10 System Recovery Options.

If your computer's system is severely damaged and you cannot access the System Recovery Options menu on your computer, you can access it using the Windows 7 installation disc or a system repair disc you created earlier. To use this method, you need to restart (boot) your computer using the disc.

1. Insert the repair disc.
2. Restart your computer using the computer's power button and boot the repair disc. You might need to press a key to boot from the disc and might have to configure your BIOS to boot from the disc.
3. Choose your language settings and then click **Next**.
4. If you are using the Windows installation disc, click **Repair your computer**.
5. Select the Windows installation you want to repair and then click **Next**.
6. On the System Recovery Options menu, click a tool to open it.

A System recovery disc is used to boot your computer if you must recover Windows from a serious error or to restore your computer.

To create a system repair disc in Windows 7, do the following:

1. Click **Start, All Programs, Maintenance, Create a System Repair Disc**.
2. Insert a CD/DVD into the drive and click **Create disc**.

The options in the system repair include

- ▶ **Startup Repair:** Fixes certain problems, such as missing or damaged system files that might prevent Windows from starting correctly.
- ▶ **System Restore:** Restores your computer's system files to an earlier point in time without affecting your files, such as email, documents, or photos. If you use System Restore from the System Recovery Options menu, you cannot undo the restore operation. However, you can run System Restore again and choose a different restore point, if one exists.
- ▶ **System Image Recovery:** You need to have created a system image beforehand to use this option. A system image is a personalized backup of the partition that contains Windows and includes programs and user data, such as documents, pictures, and music.
- ▶ **Windows Memory Diagnostic Tool:** Scans your computer's memory for errors.
- ▶ **Command Prompt:** Advanced users can use Command Prompt to perform recovery-related operations and also run other command-line tools for diagnosing and troubleshooting problems.

## Windows PE Disk

As mentioned earlier in the book, the Windows Preinstallation Environment (Windows PE) 3.0 is a minimal Win32 operating system with limited services that is built on the Windows 7 kernel. It is used to prepare a computer for Windows installation, to copy disk images from a network file server, and to initiate Windows Setup. Besides being used to deploy operating systems, it is an integral component in recovery technology with Windows Recovery Environment (Windows RE). Some of the tools included in the Windows PE disk include

- ▶ **BCDBoot:** A tool used to quickly set up a system partition or to repair the boot environment located on the system partition.
- ▶ **BCDEdit:** A command-line tool for managing the BCD Store, which describes the boot application and boot application settings, such as the boot menu.
- ▶ **BootSect:** Used to restore the boot sector on your computer.
- ▶ **Deployment Image Servicing and Management (DISM):** Used to service Windows images offline before deployment.

- ▶ **DiskPart:** Text-mode command interpreter to manage disks, partitions, and volumes.
- ▶ **DrvLoad:** Adds out-of-box drivers.
- ▶ **OscdImg:** A command-line tool for creating an image file (.iso) of a customized 32-bit or 64-bit version of Windows PE.
- ▶ **Winpeshl:** Controls whether a customized shell is loaded in Windows PE or default command prompt window. To load a customized shell, create a file named Winpeshl.ini and place it in %SYSTEMROOT%\System32 of your customized Windows PE image.
- ▶ **WpeInit:** A command-line tool that initializes Windows PE each time that Windows PE boots. It installs Plug and Play devices, processes Unattend.xml settings, and loads network resources.
- ▶ **WpeUtil:** A command-line tool that enables you to run various commands in a Windows PE session.

For more information about Windows PE and its tools, visit the following websites:

[http://technet.microsoft.com/en-us/library/cc749538\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc749538(WS.10).aspx)

[http://technet.microsoft.com/en-us/library/cc749055\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc749055(WS.10).aspx)

[http://download.microsoft.com/download/5/b/5/5b5bec17-7ea71-4653-9539-204a672f11cf/WindowsPE\\_tech.doc](http://download.microsoft.com/download/5/b/5/5b5bec17-7ea71-4653-9539-204a672f11cf/WindowsPE_tech.doc)

## Problem Steps Recorder

You can use Problem Steps Recorder to automatically capture the steps you take on a computer, including a text description of where you clicked and a picture of the screen during each click (called a screen shot). After you capture these steps, you can save them to a file that can be used by a support professional or someone else helping you with a computer problem.

When you record steps on your computer, anything you type is not recorded. If what you type is an important part of re-creating the problem you're trying to solve, use the comment feature described later in the chapter to highlight where the problem is occurring.

To record and save steps on your computer, do the following:

1. Click the **Start** button and search for **problem steps recorder** in the Search Programs and Files text box. When it finds record steps to reproduce a problem, select the link under Control Panel.

2. Click **Start Record**, as shown in Figure 16.11.
3. On your computer, go through the steps on your computer to reproduce the problem. You can pause the recording at any time and then resume it later.
4. Click **Stop Record**.
5. In the Save As dialog box, type a name for the file and then click **Save** (the file is saved with the .zip filename extension).
6. To view the record of the steps you recorded, open the .zip file you just saved and then double-click the file. The document opens in your browser.

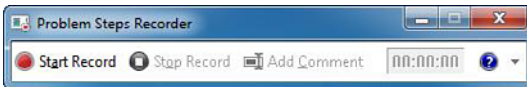


FIGURE 16.11 Problem Steps Recorder.

After recording and saving a .zip file, click the help down arrow and then click **Send to E-mail recipient**. This opens an email message in your default email program with the last recorded file attached to it. Note: You won't be able to click the Send to E-mail recipient option until you've recorded and saved a file.

When you want to add a comment, click **Add Comment**. Use your mouse to highlight the part of the screen that you want to comment on, type your text in the Highlight Problem and Comment box, and then click **OK**.

If you select the down arrow, you can configure the recorder settings. If you don't want to capture the screen shots along with each click that you performed, select **No**. This might be a consideration if you are taking screen shots of a program that contains personal information, such as bank statements, and you are sharing the screen shots with someone else.

The default is 25 screens, but you can increase or decrease the number of screen shots. Problem Steps Recorder only records the default number of screen shots. For example, if you took 30 screen shots during a recording but only had 25 screen shots as the default, the first five screen shots would be missing. In this case, you would want to increase the number of default screen shots.

---

## Cram Quiz

1. Which tool can you use to increase the number of processors used during boot?
  - A. Computer Management Console
  - B. System Information
  - C. System Configuration
  - D. IIS
2. Windows fails to start. What can you use to load the minimal set of Windows drivers and services so that you can troubleshoot the problem?
  - A. Safe Mode
  - B. WinPE
  - C. Windows Backup
  - D. System Information
3. What tool can be used to thoroughly test memory?
  - A. Computer Management Console
  - B. System Information
  - C. Memory Diagnostic tool
  - D. Safe Mode

## Cram Quiz Answers

1. **C** is correct. To increase the performance during bootup, you can select Windows to use multiple processors (assuming your system has multiple processors) by starting System Configuration, clicking the **Boot** tab, and clicking the **Advanced Options** button. Answer A is incorrect because the Computer Management Console includes multiple Microsoft Management Consoles but none that allows you to modify the number of processors used during boot. Answer B is incorrect because System Information is used view the configuration of Windows. Answer D is incorrect because IIS, short for Internet Information Services, is Microsoft's web server.
2. **A** is correct. Safe Mode starts Windows with a minimal set of drivers and services. While in Safe Mode, you can access the Control Panel, Device Manager, Event Viewer, System Information, Command Prompt, and Registry Editor. Answer B is incorrect because although WinPE is a very useful troubleshooting tool, it does not load the Windows minimal set of drivers and services. Answer C is incorrect because Windows Backup is used to back up and restore data, not to specify what is loaded during bootup. Answer D is incorrect because System Information is a tool used to view a system's configuration.

- 3. C** is correct. Windows 7 has multiple diagnostic tools, including a Memory Diagnostic tool and Network Diagnostic tool. The Memory Diagnostic tool can diagnose physical memory, including memory leaks and failing memory. Answer A is incorrect because the Computer Management Console has multiple MMC add-ins that help you manage your computer. Answer B is incorrect because the System Information gives you a single place to look to see what computer hardware and software a computer has. Answer D is incorrect because Safe Mode is a bootup option that loads minimum drivers and services, primarily used for troubleshooting and fixing boot problems.

---

# Backups and System Recovery

- ▶ **Configure backup**
- ▶ **Configure file recovery options**
- ▶ **Configure system recovery options**

## CramSaver

1. What technology is used with NTFS volumes to automatically make extra copies of data files?
  - A.** Shadow Copy
  - B.** IIS
  - C.** Windows Backup
  - D.** Msconfig
  
2. What program do you use to quickly restore your computer's system files to an earlier point in time without affecting your data?
  - A.** System Restore
  - B.** Shadow Copy
  - C.** System Image Backup
  - D.** Safe Mode

## Answers

1. **A** is correct. Shadow copies (introduced in Windows Server 2003), when configured, automatically create backup copies of the data stored in data folders on specific drive volumes at scheduled times. The drive volume must be formatted as NTFS. Windows 7 utilizes Shadow copies to provide previous versions of files even if they have never been backed up. Answer B is incorrect because IIS, short for Internet Information Services, is Microsoft's web server. Answer C is incorrect because Windows Backup must be manually executed or scheduled. Answer D is incorrect because System Configuration (MSConfig) is used to troubleshoot boot problems.
2. **A** is correct. System Restore helps you restore your computer's system files to an earlier point in time. It's a way to undo system changes to your computer without affecting your personal files, such as email, documents, or photos. Answer B is incorrect because Shadow Copy is used to provide previous versions of data files. Answer C is incorrect because the System Image Backup is a copy of the system drives required for Windows to run. Answer D is incorrect because Safe Mode is used to load only the minimum drivers and services for Windows 7 to run.

If you have been working with computers long enough, you know that no matter what you do, computers eventually fail, which causes a loss or corruption of data. Therefore, you need to take additional steps to recover your data. You should also know that the best method for data recovery is backup, backup, backup. By using Windows Backup, you can perform backups, and when it is necessary, perform restores to recover damaged or lost files, or repair corrupted system settings.

## Backup Overview

Data is the raw facts, numbers, letters, or symbols that the computer processes into meaningful information. Examples of data include a letter to a company or a client, a report for your boss, a budget proposal of a large project, or an address book of your friends and business associates. Whatever the data is, you can save it (or write it to disk) so that you can retrieve it at any time, you can print it on paper, or you can send it to someone else over the telephone lines.

Data stored on a computer or stored on the network is vital to the users and probably the organization. The data represents hours of work and is sometimes irreplaceable. Data loss can be caused by many things, including hardware failure, viruses, user error, and malicious users. When disaster occurs, the best method to recover data is backup, backup, backup. When disaster has occurred and the system does not have a backup of its important files, it is often too late to recover the files.

A backup of a system is to have an extra copy of data and/or programs. As a technician, consultant, or support person, you need to emphasize at every moment to back up on servers and client systems. In addition, it is recommended that the clients save their data files to a server so that you have a single, central location to back up. This might go as far as selecting and installing the equipment, doing the backup, or training other people in doing the backup. When doing all of this, be sure to select the equipment and method that assures that the backup is completed on a regular basis. Remember that if you have the best equipment and software but no one completes the backup, the equipment and software is wasted.

**THE BEST METHOD FOR DATA PROTECTION AND RECOVERY IS BACKUP, BACKUP, BACKUP.**

When developing for a backup, three steps should be followed. They are as follows:

1. Develop a backup plan.



2. Stick to the backup plan.
3. Test the backup.

When developing a backup plan, you must consider the following:

- ▶ What equipment will be used?
- ▶ How much data needs to be backed up?
- ▶ How long will it take to do the backup?
- ▶ How often must the data be backed up?
- ▶ When will the backup take place?
- ▶ Who will do that backup?

Whatever equipment, person, or method is chosen, you must make sure that the backup will be done. If you choose the best equipment, the best software, and the brightest person, and the backup is not done for whatever reason, you wasted your resources and you put your data at risk.

How often the backup is done depends on the importance of the data. If you have many customers loaded into a database, which is constantly changed, or your files represent the livelihood of your business, you should back them up everyday. If there are a few letters that get sent throughout the week with nothing vitally important, you can back up once a week.

## Types of Backups

All types of backups can be broken into the following categories:

- ▶ **Normal/Full:** The full backup backs up all files selected and shuts off the archive file attribute, indicating the file has been backed up.
- ▶ **Incremental:** An incremental backup backs up the files selected if the archive file attribute is on (files since the last full or incremental backup). After the file has been backed up, it shuts off the file attribute to indicate that the file has been backed up. Note: You should not mix incremental and differential backups.
- ▶ **Differential:** A differential backup backs up the files selected if the archive file attribute is on (files since the last full backup). Different from the incremental backup, it does not shut off the archive attribute. Note: You should not mix incremental and differential backups.

- ▶ **Copy backup:** A copy backup is like a normal backup, but it does not shut off the archive attribute. This is typically used to back up the system before you make a major change to the system. The archive attribute is not shut off so that your normal backup procedures are not affected.

You decide to back up the entire hard drive once a week on Friday. You decide to use the full backup method. Therefore, you perform a full backup every Friday. If the hard drive goes bad, you use the last backup to restore the hard drive.

You decide to back up the entire hard drive once a week on Friday. You decide to use the incremental method. Therefore, you perform a full backup on week 1. This shuts off all of the archive attributes, indicating that all of the files have been backed up. On week 2, week 3, and week 4, you perform incremental backups using different tapes or disks. Because the incremental backup turns the archive attribute, it backs up only new files and changed files. Therefore, all four backups make up the entire backup. It is much quicker to back up a drive using an incremental backup than a full backup. Of course, if the hard drive fails, you must restore backup #1, backup #2, backup #3, and backup # 4 to restore the entire hard drive.

After the backups are complete, you should check to see if the backups actually worked. You can do this by picking a nonessential file and restoring it to the hard drive. This helps discover if the backups are empty or a backup/restore device is faulty.

You should keep more than one backup. Tapes and disks do fail. One technique is to rotate through three sets of backups. If you perform a full backup once a week, you would then use three sets of backup tapes or disks. During week 1, you use tape/disk #1. During week 2, you use tape/disk #2, and during week 3, you use tape/disk #3. On week 4, you start over and use tape/disk #1. If you have to restore a hard drive and the tape or disk fails, you can always go to the tape or disk from the week before. In addition, you should perform monthly backups and store them elsewhere. You might be surprised how many times a person loses a file but does not realize it for several weeks. If the data is important enough, you might consider keeping a backup set in a fireproof safe offsite. Lastly, when a system is initially installed and when you make any major changes to the system's configuration, it is always recommended to make two backups before proceeding. This way, if anything goes wrong, you have the ability to restore everything to the way it was before the changes. The reason for the two backups is that tapes have been known to go bad on occasion.

Some places use the Grandfather, Father, Son (GFS) backup rotation, which requires 21 tapes based on a five-day rotation. Each month, you create a grandfather backup, which is stored permanently offsite, never to be reused. Each week, you create a full weekly backup (father), and each day you create a differential or incremental backup (son).

After completing a backup, you should properly label the tape or disk before removing it and then store the tape and disk to a secure, safe place. In addition, you should keep a log of what backups have been done. The log keeps track of what was backed up and when it was backed up, which is especially useful if you need to rebuild the server. It also lets you know if someone is forgetting to do the backup.

## Backup and Restore Center

To back up your drives and files, you can use the Backup and Restore Center. To access the Backup and Restore Center, do the following:

1. Click the **Start** button, click **All Programs**, click **Maintenance**, and click **Backup and Restore**.
2. To set a backup, click the **Set up backup** link.
3. Specify where you want to store your backups. You can specify a secondary drive or the network and click **Next**.
4. You can let Windows choose your files or you can choose your files.
5. If you choose what to back up, you can include what drives and folders you want to back up. The System drives are automatically chosen, as shown in Figure 16.12.
6. Review your settings and click the **Save settings and run backup** button.

You can make a backup at any time by clicking the **Back up now** button. You can also schedule a backup, including configuring a recurring backup that backs up on a regular basis. You can then use the options at the bottom of the window to restore user files, system settings, or all files, as shown in Figure 16.13.

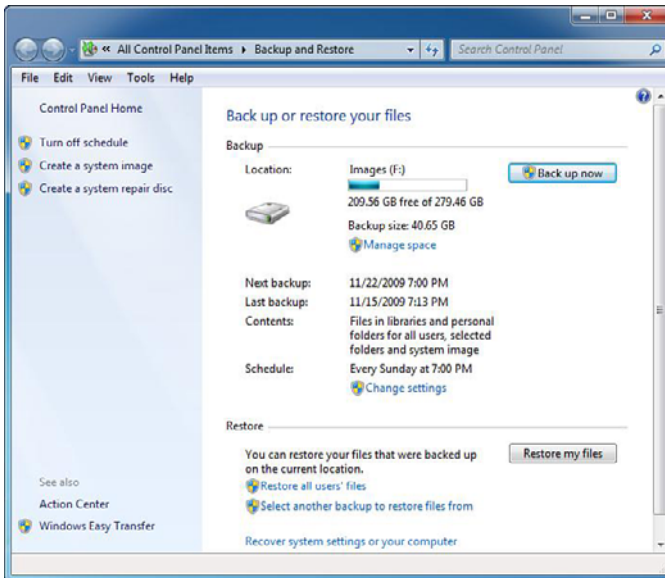


FIGURE 16.12 Choosing what to back up.

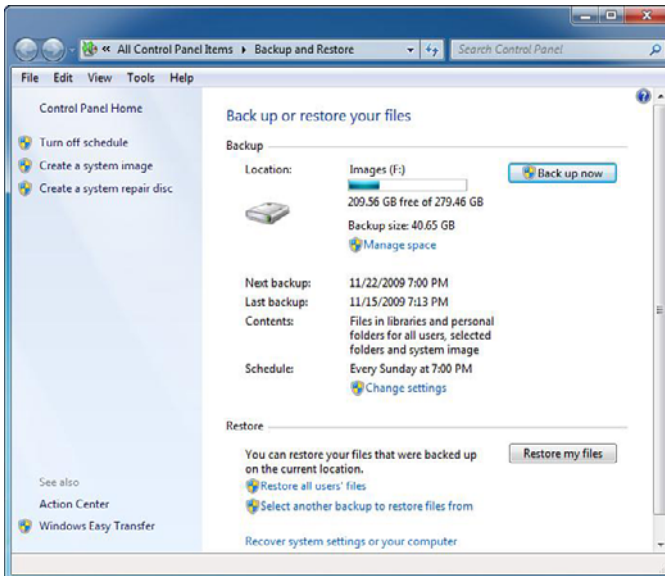


FIGURE 16.13 Backup and Restore Center.

## System Image Backup

A System Image Backup, sometimes referred to as the Complete PC Backup, is a copy of the system drives required for Windows to run, and it is one of the fastest ways to restore your hard disk. It can also include additional drives. It is an exact copy of the disk or volume at the time the image was made (cluster by cluster). Because it is an exact copy, it can be used to restore your computer, including all configuration settings and files, if your hard disk or computer stops working. You can create a system image by clicking **Create a system image** in the Backup and Restore Center.

## System Protection

System protection is a set of features that regularly creates and saves information about your computer's system files and settings (System Restore) and saves previous versions of files that you've modified. It saves these files in restore points, which are created just before significant system events, such as the installation of a program or device driver. They're also created automatically once every seven days if no other restore points were created in the previous seven days, but you can create restore points manually at any time.

## System Restore

System Restore helps you restore your computer's system files to an earlier point in time. It's a way to undo system changes to your computer without affecting your personal files, such as email, documents, or photos. This comes in handy when you install a program or a drive that causes Windows to behave unpredictably. If uninstalling does not fix the problem, you can try restoring your computer's system to an earlier date when everything worked correctly.

Restore points are created automatically every day and also just before significant system events, such as the installation of a program or device driver. You can also create a restore point manually. The System restore points back up the following settings:

- ▶ Registry
- ▶ DLLcache folder
- ▶ User profile
- ▶ COM+ and WMI information
- ▶ IIS metabase
- ▶ Certain monitored system files

System restore points are different from data backup. It is not intended for backing up personal files. Therefore, it cannot help you recover a personal file that is deleted or damaged. You should regularly back up your personal files and important data using a backup program.

If you know you are going to make significant changes to your machine including loading drivers or programs, you should create a restore point.

When a problem occurs, you can also choose from a list of restore points. Try using restore points created just before the date and time you started noticing problems.

To configure which volumes are protected with System Restore, do the following:

1. Right-click **Computer** and choose **Properties**.
2. Click **System protection**.

If you click the drive you want to configure and click the **Configure** button, you can specify to enable or disable restore system settings or previous versions of files (explained in the next section), as shown in Figure 16.14. You can also specify how much disk space you want to allocate toward system protection and delete any restore points if you are low on disk space. You can also manually create a restore point by clicking the Create button.

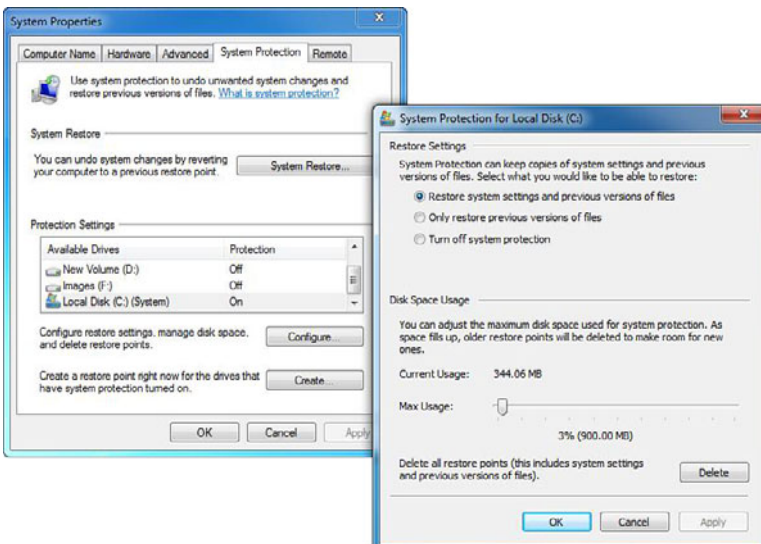


FIGURE 16.14 Configuring System Protection.

To access the System Restore utility, do the following:

1. Click the **Start** button and select **All Programs**.
2. Select **Accessories**.
3. Select **System Tools**.
4. Select **System Restore** to see the screen shown in Figure 16.15.
5. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

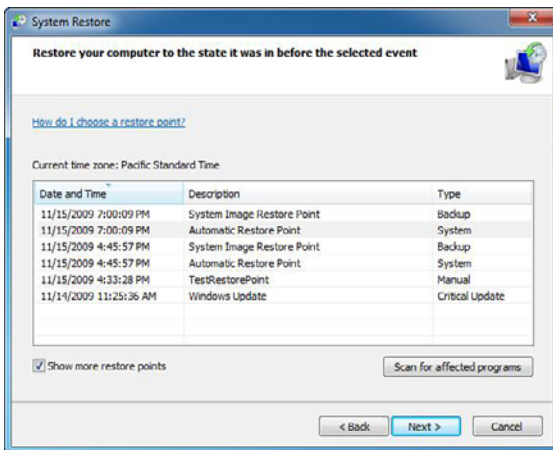


FIGURE 16.15 System Restore.

## Previous Versions of Files

Shadow copies, introduced in Windows Server 2003, when configured, automatically create backup copies of the data stored in data folders on specific drive volumes at scheduled times. The drive volume must be formatted as NTFS. Windows 7 utilizes Shadow copies to provide previous versions of files even if they have never been backed up.

With Windows 7, Shadow Copy is automatically turned on as part of System Restore and creates copies on a scheduled basis of files that have changed. It works on single files as well as whole folders. If you right-click a data folder or individual file and click **Properties**, you can then click the **Previous Versions** tab to view and restore individual files, as shown in Figure 16.16.

### Note

Because this only backs up periodically, it does not keep individual documents if you change the document several times in a short period of time.

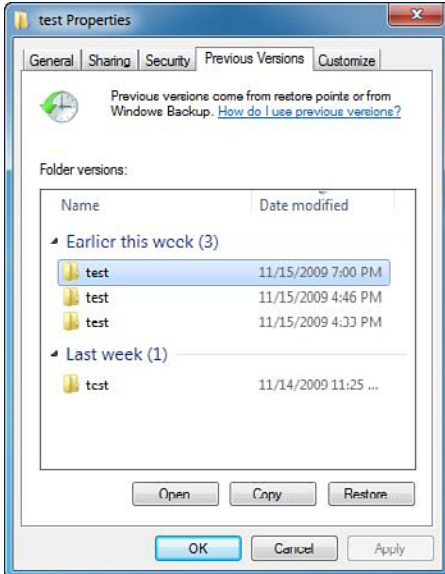


FIGURE 16.16 Previous versions of a folder or file.

## Removing Restore Points and Previous Versions of Files

The Disk Cleanup utility was introduced in Chapter 4, “Disk Management.” It removes temporary files, empties the Recycle Bin, and removes a variety of system files and other items that you no longer need. After you scan your disk using the Disk Cleanup utility, you can click the **More Options** tab and click the **Clean up** button in the System Restore and Shadow Copies section to delete all but the most recent restore point on the disk, including previous versions of files.



---

## Cram Quiz

1. You are going to upgrade a couple of applications and you want to back up all system and data files. What should you use?
  - A. Create a System Image Backup
  - B. Use System Restore
  - C. Use Previous Versions of Files
  - D. Use System Configuration
2. Which of the following does System Restore NOT back up?
  - A. Registry
  - B. COM+ and WMI information
  - C. IIS metabase
  - D. Data files created by a user

## Cram Quiz Answers

1. **A** is correct. A System Image Backup, sometimes referred to as the Complete PC Backup, is a copy of the system drives required for Windows to run and is one of the fastest ways to restore your hard disk. It can also include additional drives. Answer B is incorrect because System Restore only backs up System files, not data files. Answer C is incorrect because the Previous Versions of Files only backs up data files, not system files. Answer D is incorrect because System Configuration is a troubleshooting tool for boot problems, not a backup tool.
2. **D** is correct. System Restore backs up the registry, DLL cache folder, user profiles, COM+ and WMI information, IIS metabase, and certain monitored files. It does not back up data files.

# Review Questions

1. You work as the desktop support technician at Acme.com. You have a user that loaded a driver but now Windows does not boot properly. You want to display the driver names while they are being loaded during startup. What should you do?
  - A. Start System configuration. On the Boot tab, select the Base video checkbox.
  - B. Start System configuration. On the Boot tab, you should select the Boot log checkbox.
  - C. Start System configuration. On the Boot tab, you should select the No GUI boot checkbox.
  - D. Start System configuration. On the Boot tab, select the OS boot information checkbox.
2. You work as the desktop support technician at Acme.com. You have a user who reports experiencing slowness problems over the last few weeks. You need to identify the cause of the failures. Therefore, you want to look at the historical view of workstation performance and see when the failures first started. What should you do?
  - A. Make use of Performance Monitor
  - B. Make use of the Reliability Monitor
  - C. Make use of a System Diagnostics Data Collector Set
  - D. Make use of the Resource Overview tool
3. You work as the Help Desk technician at Acme.com. You have a user who is getting a Stop error when the computer is started in Normal mode or Safe Mode. What should you do to troubleshoot this problem further?
  - A. Uninstall Windows 7 and reinstall the previous version of Windows
  - B. Reboot the computer using the Windows 7 installation DVD and run the Startup Repair tool
  - C. Run Software Explorer
  - D. Disable startup items by running Msconfig.exe
4. You make changes to the video refresh rate on your computer and now the display does not work properly. What should you do?
  - A. Run the SYSEDIT tool
  - B. Reinstall Windows
  - C. Reboot the system with the emergency repair disk
  - D. Press **F8** during the boot sequence and select Last Known Good Configuration

5. Your machine does not boot properly. You suspect a faulty driver that you just installed. Unfortunately, you cannot access the Device Manager because the system does not complete the boot process. What should you do next?
- A. Restart the computer with another version of Windows
  - B. Insert a DOS bootable disk into the drive and boot the system
  - C. Reboot the computer in Safe Mode
  - D. Start the System Configuration tool
6. What tool would you use to temporarily disable a service that starts during the boot process?
- A. Device Manager
  - B. System Configuration
  - C. Boot.ini tool
  - D. Last Known Configuration option
7. You just loaded a new application. Now your computer has gotten slow and sometimes causes Stop errors. Even after reinstalling the application, you still have the same problems. What can you try next?
- A. Roll back the latest driver using Device Manager
  - B. Reboot the computer in Safe Mode
  - C. Press **F8** during the boot sequence and select Last Known Good Configuration
  - D. Use the System Restore to restore to a known good working restore point
8. Which type of backup can you perform using the Windows 7 Backup and Restore program if you only want to back up files that have their archive bits set and you want the backup job to clear each file's archive bit after each file has been backed up?
- A. Incremental
  - B. Differential
  - C. Normal
  - D. Copy

9. You have a computer running Windows 7 with a C and D drives. Both hard drives are formatted with the NTFS file system. What do you need to disable the previous versions on the D drive?
- A. Modify the Quota settings
  - B. Modify the Sharing settings
  - C. Use the Disk Management snap-in
  - D. Modify the System Protection settings from System Properties
10. What can you use to delete all System Protection snapshots on a computer running Windows 7?
- A. Run Disk Defrag
  - B. Run Disk Cleanup for System Restore and Shadow copies
  - C. Restore files from Previous Versions
  - D. Restore files using System Restore

## Review Question Answers

1. Answer **D** is correct. If you open System Configuration, select the Boot tab, and select OS boot information, it shows you the driver names that are loaded during startup. Answers A, B, and C are incorrect because those options do not provide that information. Base video starts the monitor with a 640 × 480 resolution. The Boot log generates a log that could be accessed after it boots. The No GUI boot checkbox starts in with a command prompt.
2. Answer **B** is correct. The two places to look for a history of problems are the Event Viewer and the Reliability Monitor. Answer A is incorrect because Performance Monitor is used to measure performance. Answer C is incorrect because the Data Collector Set is used to group counters together so that you can call them up as needed or schedule them to be measured. Answer D is incorrect because the Resource Overview tool shows the performance of the major subcomponents, including CPU, memory, network, and disk.
3. Answer **B** is correct. Because you cannot start the computer, there might be a problem with the startup files. Therefore, you need to run the Startup Repair tool. Answer A is incorrect because you don't want to go back to an old operating system. Answers C and D are incorrect because you cannot start Windows to get to the Software Explorer or msconfig.exe (System Configuration tool).

4. Answer **D** is correct. If you load a driver and your machine does not boot properly, you can access the advanced boot menu and try Last Known Good Configuration. Answer A is incorrect because you cannot access Windows to use SYSEDIT. Answer B is incorrect because reinstalling Windows takes a lot of effort and might not correct the problem. Answer C is incorrect because there is no emergency repair disk to use with Windows 7; everything is included with the Windows 7 installation disk.
5. Answer **C** is correct. If you cannot boot the computer, the next logical step is to boot Windows in Safe Mode. In Safe Mode, minimum drivers are loaded. Answer A is not a viable option because most systems do not have another hard drive with another version of Windows. This solution can also become very messy. Answer B is incorrect because you cannot use DOS to correct most Windows problems. Answer D is incorrect because you need to first load Windows before you can use the System Configuration tool.
6. Answer **B** is correct. The system configuration tool is a diagnostic tool that can help you isolate startup programs and services that prevent Windows from booting. Answer A is incorrect because Device Manager manages devices, not services. Answer C is incorrect because there is no such thing as the boot.ini tool or file in Windows 7. Answer D is used to revert back when you load a driver, service, or program that prevents Windows from loading. It does not disable a service.
7. Answer **D** is correct. System Restore can reconfigure Windows to its original settings before the problem occurred. Answer A is incorrect because this is not a device problem. Answer B is incorrect because you can load Windows, so you don't need to use Safe Mode. Answer C is incorrect because if you log in to Windows successfully, you overwrite the Last Known Good Configuration.
8. Answer **A** is correct. When you complete an incremental backup, you are backing up all new and changed files since the last backup. Answer B is incorrect because differential backups do not shut off the archive attribute. Answer C is incorrect because the normal or full backup copies all files regardless of the archive attribute. Answer D is incorrect because the Copy command backs up all files but does not shut off the archive attribute.
9. Answer **D** is correct. To enable or disable what is affected by System Restore and Previous Versions, you must use the System Protection settings from System Properties. Answer A is incorrect because the Quota settings are used to limit how much space a user can use on a system. Answers B and C are incorrect because you cannot use System Protection from the Sharing properties or Disk Management snap-in.
10. Answer **B** is correct. Disk Cleanup enables you to remove old copies of System Restore and Shadow copies. Answer A is incorrect because the Disk Defrag is used to optimize a disk by putting files back together on a disk, allowing for quicker access time. Answer C is incorrect because restoring files or reverting to an earlier snapshot does not remove old copies of the System Restore or Shadow copies.

# Practice Exam

This element consists of 50 questions that are representative of what you should expect on the actual exam. The questions here are multiple choice, however, and not simulations because of the limitations of paper testing. Still, this exam should help you determine how prepared you are for the real exam and provide a good base for what you still need to review. As you take this exam, treat it as you would the real exam: Time yourself (about 90 minutes), and answer each question carefully, marking the ones you want to go back to and double check. The answers and their explanations are at the end of the exam.

1. Which of the following describes Windows Aero?
  - A. A new hardware-based graphical user interface intended to be cleaner and more aesthetically pleasing than those of previous versions of Windows
  - B. A special theme that is based on the aerospace industry
  - C. A background theme that shows the blue skyline
  - D. A search-oriented desktop interface
  
2. You work as a desktop support technician at Acme.com. Because you need to connect to the domain, you need to install Windows 7 Professional Edition on a computer for the graphics department. The computer has the following specifications:
  - ▶ 1.5 GHz AMD processor
  - ▶ 2 GB of RAM
  - ▶ Drive C (system drive) has 15 GB of free disk space
  - ▶ Drive D (program drive) has 60 GB of free disk space
  - ▶ Integrated sound card
  - ▶ Intel 10/100 network adapter

Which hardware does not meet the minimum requirements to install Windows 7?

- A. You should add a faster processor to the computer.
- B. You should add more memory to the computer.
- C. You need to free up space on drive C.
- D. You should install Windows 7 on drive D.

3. You are the network administrator for Acme.com. You have ordered some new computers and the new computers only have one partition with Windows 7 Home Basic. Unfortunately, each computer must be running Windows 7 Professional Edition so that they can connect to the Windows domain. When you upgrade Windows 7, which directory holds the old operating system files and directories in case you need to access to the Documents and Settings folders and Program Files folder?
- A. Windows\panther folder
  - B. Windows folder
  - C. Windows.OLD folder
  - D. Files and Settings folder
  - E. Explorer folder
4. If you want to migrate user settings from a Windows Vista computer, which parameter should you use with the ScanState.exe command?
- A. /vista
  - B. /target:vista
  - C. /targetvista
  - D. No options are required.
5. You have an offline Windows 7 image of a reference computer. What program can you use to perform an offline installation of language packs specified in an answer file?
- A. The `imagex` command-line utility
  - B. The `pkgmgr.exe` utility
  - C. The Windows SIM
  - D. The DISM tool
6. How many primary partitions without an extended partition can reside on a basic MBR disk under Windows 7?
- A. 3
  - B. 4
  - C. 1
  - D. 128
7. You want to assign an address to a computer that will be available on the Internet, and it will have the same address for both IPv4 and IPv6. What kind of address is this?
- A. A unique private address
  - B. A multicast local address

- C. A site-local address
  - D. A global unicast address
8. Which authentication protocol is used for backward compatibility with pre-Windows 2000 operating systems?
- A. Kerberos
  - B. Windows NT LAN Manager
  - C. Certificate mappings
  - D. Password Authentication Protocol
9. You work as part of the IT support staff at Acme.com. You have upgraded several computers from Windows XP Professional to Windows Vista Enterprise to Windows 7 Enterprise. You had an accounting application that worked fine in Windows XP but does not run fine on Windows 7. After further research, you find when the user tries to run the application, it asks for a login. When the user uses a standard user account, the application fails, but when you use an administrator user account and password, the application works. What is the best solution to fix this problem?
- A. Add the user accounts to the local administrator group.
  - B. Add the user accounts to the domain administrator group.
  - C. Use Parental Control for the users to access the applications.
  - D. Right-click the executable and select Properties. Use the application's Properties dialog box to run this program as an administrator.
10. What is used to help you identify fake websites that are made to look like legitimate websites?
- A. Protected Mode
  - B. Phishing filter
  - C. Add-on Manager
  - D. Digital signature
11. You have purchased some devices that have been sitting on the shelf at a store for several months and are about ready to be discontinued. You installed the drivers for those devices and now your system has some sporadic errors. What should you do?
- A. Look on the Windows DVD for more up to date drivers
  - B. Check with the manufacturer's website and the Windows update website for more up-to-date drivers
  - C. Upgrade Windows 7 to the Ultimate edition so that it can make proper use of the drivers
  - D. Disable the prompting of unsigned driver warnings



- 12.** You have a new computer with Windows 7 on it. When you visit certain websites using Internet Explorer, you click on the links and nothing happens. What is the problem?
- A.** You have been denied access to the website by the network administrator.
  - B.** The website has been taken offline.
  - C.** The links generate pop-up windows, which are blocked by default.
  - D.** The website is not on your trusted list.
- 13.** You have Windows 7 loaded on a computer with one primary volume that holds Windows, your applications, and your data files. What happens if the C drive starts to run out of disk space? (Choose all that apply.)
- A.** Your computer runs slower.
  - B.** Your machine is less reliable.
  - C.** If you attempt to move files from one location to another drive, such as a USB drive, Windows might say that you are out of disk space.
  - D.** Windows shifts into compression mode to save disk space.
- 14.** You have a user that made some changes to the advanced options in Internet Explorer. Unfortunately, the user cannot access certain websites. What can you do to reset those options?
- A.** Reinstall Internet Explorer
  - B.** Navigate to the Advanced tab in Internet Options and click Restore advanced settings
  - C.** Navigate to the Advanced tab in Internet Options and click Reset
  - D.** Navigate to the Security tab in Internet Options and click Reset all zones to default level
- 15.** How do you turn off the prompts generated by User Account Control? (Choose two answers.)
- A.** Use local or group policies
  - B.** Click the Turn User Account Control Off link under User Accounts
  - C.** Use the Computer Management console
  - D.** Open the System properties of the computer and click the Turn Off button under the UAC
- 16.** You have more than 50 laptop computers that are running Windows 7 Enterprise Edition that you need to connect to your corporate wireless network. What is the easiest way to do that?
- A.** Log in to each computer and manually configure the wireless settings

- B. Copy the wireless settings to a shared folder and then copy the wireless settings to each computer
  - C. Save the wireless network settings to a USB flash drive and use that flash drive on each computer to copy the configuration
  - D. Use the Autodetect feature of Windows 7 to detect the wireless settings
  - E. Use group policies to automatically configure the wireless settings
17. You think some of your boot files have gotten corrupted, resulting in improper loading of Windows 7. What can you do to fix the problem?
- A. Start safe mode and run further diagnostics to figure out which file is causing the problem.
  - B. Insert the Windows 7 installation disc using the Startup Repair Tool to fix the problem.
  - C. Insert the Windows 7 installation disc and start Windows in safe mode.
  - D. Insert the Windows 7 installation disc and start Windows from the DVD. Then run further diagnostics to figure out which file is causing the problem.
18. A user from your office has reported some strange errors. Where can you look at the logs to see if they report some of the errors?
- A. Log Trace in Administrative Tools
  - B. Event Viewer in the Computer Management console
  - C. Logging in the Control Panel
  - D. Debugging Logs in Administrative Tools
19. Which of the following are not TCP/IP private addresses?
- A. 10.1.2.50
  - B. 172.16.23.42
  - C. 172.32.34.202
  - D. 192.168.4.5
20. You have several laptops that you are trying to make as secure as possible in the event that they are stolen. What should you implement to protect their entire volumes?
- A. NTFS
  - B. Share permissions
  - C. BitLocker
  - D. EFS

21. You suspect that a program that you started is using too much memory. How can you verify this?
- A. Use the Event Viewer
  - B. Use the Task Manager
  - C. Use the Computer Management console
  - D. Use the Windows Defender
22. Which utility would you use to prepare an installed system so that its image could be copied to multiple computers?
- A. imagex
  - B. setup
  - C. diskpart
  - D. sysprep
23. You are looking at the Device Manager. You see a device that has a down arrow on it. What is the problem?
- A. The device is having a problem.
  - B. The device is disabled.
  - C. The device is sleeping.
  - D. The device is not connected.
24. What command can be used to show network connectivity to a computer?
- A. ipconfig
  - B. arp
  - C. ping
  - D. nslookup
25. Which of the following will you not find in the Windows Mobility Center?
- A. Brightness
  - B. Battery Status
  - C. Pointer Devices
  - D. Presentation Settings
26. What do you call an XML file that scripts the answers for a series of GUI dialog boxes and other configuration settings used to install Windows?
- A. Answer file
  - B. Installation script
  - C. Windows image
  - D. Catalog

27. Which utility would you use to migrate the files and settings to removable media or to a network share and later restore the files and settings to the target computer?
- A. Windows Easy Transfer
  - B. User State Migration Tool
  - C. Windows PE
  - D. Sysprep
28. You are a desktop technician for Acme.com. You have 20 different computers used by your company. You want to quickly check to see if they support a Windows 7 installation. What utility can you use to easily determine their capability to run Windows 7?
- A. Run the Windows 7 Upgrade Advisor
  - B. Run the System Checker program
  - C. Run the System Information program
  - D. Run the Computer Management console
29. Which utility would you use to manage the volumes on your system?
- A. Disk management applet in the Control Panel
  - B. Computer Management console found in administrative tools
  - C. Disk administrator found on the desktop
  - D. Disk runner found in My Computer
30. When you run a new application, you get a warning saying User Account Control stops unauthorized changes to your computer and that your computer needs your permission to continue. What should you do when you get this warning?
- A. You need to determine if the application comes from a reliable source. If it does, click the Continue button.
  - B. You need to verify the NTFS permissions for the application.
  - C. You need to run the application as an administrator.
  - D. You need to log out and log in as an administrator and retry the application again.
31. Besides allowing and blocking programs from communicating over the Internet and blocking ports to communicate, what else would you use the Windows Firewall with Advanced Security console for?
- A. To monitor network traffic
  - B. To configure IPsec
  - C. To view network attacks
  - D. To manage your anti-virus program
  - E. To manage your anti-spyware program

- 32.** What does Protected Mode in Internet Explorer do?
- A.** Prevents Component Object Model (COM) objects, such as ActiveX controls, from automatically modifying files and settings
  - B.** Helps stop phishing websites
  - C.** Helps stop viruses from infecting your computer
  - D.** Helps prevent packet sniffing on the network
- 33.** What would you use to check for but not fix errors on Drive D?
- A.** Run the `chkdsk D:` command at the command prompt
  - B.** Run the `chkdsk D: /f` command at the command prompt
  - C.** Run the `scandisk D:` command at the command prompt
  - D.** Run the `scandisk D: /F` command at the command prompt
  - E.** Right-click the D drive and select Error-Checking
- 34.** ReadyBoost and ReadyDrive increase performance on your machine. What is the difference between the two? (Choose two answers.)
- A.** Windows ReadyBoost uses USB flash devices as additional sources for caching.
  - B.** Windows ReadyDrive uses hybrid drives on laptop computers.
  - C.** Windows ReadyBoost uses hybrid drives on laptop computers.
  - D.** Windows ReadyDrive uses USB flash devices as additional sources for caching.
- 35.** You loaded a new video card driver, which now causes your machine to not boot properly. What can you do to correct this problem?
- A.** Boot to VGA mode (Base Video) and roll back the old driver
  - B.** Boot to the command prompt and roll back the old driver
  - C.** Boot with the Windows 7 DVD and run the repair
  - D.** Connect to the Windows Update website to get the correct driver
- 36.** You have a few programs that are causing some strange errors to appear when Windows starts. You want to isolate which program is generating the errors. What can you do? (Select the best answer.)
- A.** Use Parental Control to disable each program
  - B.** Use Windows Defender to temporarily disable programs
  - C.** Edit the Registry to disable each program
  - D.** Use `msconfig` and temporarily disable programs

37. Which of the following statements are true when discussing wireless technology used with Windows 7? (Choose two answers.)
- A. Personal mode provides authentication via a preshared key or password.
  - B. Enterprise mode provides authentication using IEEE 802.1X and EAP.
  - C. Enterprise mode provides authentication via a preshared key or password.
  - D. Personal mode provides authentication using IEEE 802.1X and EAP.
38. Your browser cannot find a website that you are trying to access. You eventually correct an error on the DNS server, which now knows the correct address to the website. What do you need to do to now access the website?
- A. You need to run the `ipconfig /registerdns` command.
  - B. You need to run the `ipconfig /flushdns` command.
  - C. You need to shut down your machine and restart it.
  - D. You need to change the IP address of your DNS server.
39. You have a Windows 7 computer used in the office through shared folders. You also want users to be able to remotely access the computer to run programs from that computer from their own computers by using Remote Desktop. What do you need for them to access the computer?
- A. You need to add the users to the administrator's group.
  - B. You need to add users to the Power Users group.
  - C. You need to add the users to the Remote Desktop Users group.
  - D. You need to add users to the Telnet group.
40. You have BitLocker Drive Encryption on a computer that is running Microsoft Windows 7 Enterprise Edition, which has the Trusted Platform Module (TPM) installed. When you set up the computer, you printed out the recovery password, which you keep in your files. What do you need to recover the system if a TPM error occurs and the user cannot access the data on the computer?
- A. Start the computer and enter the recovery password.
  - B. Start the computer with the USB flash drive.
  - C. Start the computer and enter the TPM management console.
  - D. Boot the computer with the Windows 7 installation disc. Enter the recovery password when you need to log in.
41. What command do you use to check what IP address is resolved for a host name?
- A. `ipconfig /dns`
  - B. `nslookup`

- C. NBTStat
  - D. resolve
42. You work as the desktop support technician at Acme.com. Pat is a member of the manager group. There is a shared folder called MANAGEMENT on an NTFS partition on a remote Windows 7 computer. Pat is given the Write NTFS permission, the Manager group is given the Read & Execute NTFS permissions and the Everyone group has the Read NTFS permission to the DATA folder. In addition, Pat, Manager, and Everyone are assigned the shared Contributor permission to the MANAGEMENT folder. When Pat logs on his client computer and accesses the MANAGEMENT folder, what are his permissions? (Choose all that apply.)
- A. Read the files in that folder
  - B. Write to the files in the folder
  - C. Execute the files in the folder
  - D. Delete the files in the folder
  - E. Have no access to the files in the folder
43. What do you call a bootable tool that replaced MS-DOS as the pre-installation environment?
- A. Windows PE
  - B. Installation script
  - C. Windows image
  - D. Catalog
44. What is the name of the answer file used on removable media when you install Windows 7?
- A. Answer.txt
  - B. Answer.xml
  - C. autoattend.xml
  - D. Install.xml
45. When discussing content zones used in Internet Explorer, what defines the Local Intranet Zone?
- A. Anything that is not assigned to any other zone and anything that is not on your computer or your organization's network
  - B. Computers that are part of the organization's network that do not require a proxy server, as defined by the system administrator
  - C. Contains trusted sites from which you believe you can download or run files without damaging your computer or data or that you consider is not a security risk

- D.** Contains sites that you do not trust from which downloading or running files might damage your computer or data or that are considered a security risk
46. When you visit several websites using Internet Explorer, additional windows appear. At times, you try to close these windows, but more windows are appearing faster than you can close them. What should you make sure you have enabled?
- A.** Phishing protection
  - B.** Dynamic protection
  - C.** Pop-up blocker
  - D.** Windows Defender
47. What is a special microchip in some newer computers that supports advanced security features, including BitLocker encryption?
- A.** ActiveX controls
  - B.** Trusted Platform Module
  - C.** Dynamic Protection
  - D.** NTFS
48. What do you use to encrypt individual files on your system?
- A.** NTFS
  - B.** Compression
  - C.** EFS
  - D.** BitLocker
49. When your machine goes into hibernate, what is the name of the file to which it saves the contents of the system memory?
- A.** page.sys
  - B.** pagefile.sys
  - C.** hiberfil.sys
  - D.** power.sys
50. You want to have events from the Event Viewer from computer1 sent to computer2. What command do you execute on computer1?
- A.** `winrm quickconfig`
  - B.** `wecutil qc`
  - C.** `tether computer2`
  - D.** `subscribe computer2`



# Answers to Exam Questions

1. Answer **A** is correct. Windows Aero is a new hardware-based graphical user interface intended to be cleaner and more aesthetically pleasing than those of previous Windows. Answers B, C, and D have nothing or little to do with the Windows Aero theme.
2. Answer **C** is correct. The system requirements specify 16 GB free hard disk space. The system in question only has 15 GB of free disk space. Of course, it is recommended that you have a much larger hard drive. Because the system requirements specify 1 GHz processor and 1 GB of RAM, Answers A and B are incorrect. Because it has been specified that Windows goes on drive C and programs go on drive D, Answer D is incorrect.
3. Answer **C** is correct. When you perform a clean installation of Windows 7 on a hard disk partition that contains an existing Windows installation (assuming you did not reformat the hard disk), the previous operating system, user data, and program files are saved to a Windows.OLD folder. Answer A is incorrect because the Windows\panther folder is used for installation logs. Answer B is incorrect because the Windows folder is where the Windows files reside. Answers D and E do not exist in a normal Windows 7 installation.
4. Answer **C** is correct. When you want to migrate from a Windows Vista computer, you should use the `/targetvista` option. Answers A and B are incorrect because `/vista` and `/target:vista` are invalid options. Therefore, the other answers are incorrect.
5. Answer **D** is correct. Deployment Image Servicing and Management (DISM) is a command-line tool that is used to service and manage Windows images. You can use it to install, uninstall, configure, and update Windows features, packages, drivers, and international settings. Answer A is incorrect because `imageex` is used to create and manage a WIM file. Answer B is incorrect because `pkgmgr.exe` (short for Package Manager) installs, uninstalls, configures, and updates features and packages for Windows. Answer C is incorrect because Windows SIM is used to create or validate answer files.
6. Answer **B** is correct. You can create up to four primary partitions on a basic disk without an extended partition. Answer A is incorrect because you are limited to three primary partitions only if there is an extended partition on the disk. Answer C is incorrect because you can have more than one primary partition on a basic disk. Answer D is incorrect because you are limited to a maximum of four primary partitions on a basic MBR disk; a basic GPT disk can host up to 128 partitions.
7. Answer **D** is correct. If you want an address to be available from the Internet and be the same address for both IPv4 and IPv6, it must have a global address that can be seen on the Internet. Answer A is incorrect because private addresses cannot be used on the public network such as the Internet. Answer B is incorrect because it has to be a single address assigned to a single computer, not a multicast local address, which is used to broadcast to multiple addresses at the same time. Answer C is incorrect because a local address cannot be seen on the outside.

8. Answer **B** is correct. Windows NT LAN Manager (NTLM) is an authentication protocol used for backward compatibility with pre-Windows 2000 operating systems and some applications. Answer A is incorrect because Kerberos is the main logon authentication method used by clients and servers running Microsoft Windows operating systems to authenticate both user accounts and computer accounts. Answer C is incorrect because certificate mappings are used with smart cards (which contain a digital certificate) for logon authentication. Answer D is incorrect because Password Authentication Protocol (PAP) is used as a remote access authentication protocol that sends the username and password in clear text (unencrypted).
9. Answer **D** is correct. To configure legacy applications to run under Windows 7, you can right-click an executable and open the Properties dialog box. From there, you can specify what environment to run under and, if necessary, specify if the application can run under an administrator account. Answer A is incorrect because adding an account to the Administrators group opens your system up as a security risk when running other applications. Answer B is incorrect because adding an account to the domain administrator group opens your system as a security risk when running other applications. Answer C is incorrect because Parental Controls are not available on domains.
10. Answer **B** is correct. The Phishing filter helps protect you from online phishing attacks, fraud, and spoofed websites. Answer A is incorrect because the Protected Mode helps protect you from websites that try to save files or install programs on your computer. Answer C is incorrect because the Add-on Manager lets you disable or allow web browser add-ons and delete unwanted ActiveX controls. Answer D is incorrect because the digital signature tells you who published a file and whether it has been altered since it was digitally signed.
11. Answer **B** is correct because it is obvious that these drivers are not the newest. Therefore, you should check the Windows update website and manufacturer websites for newer drivers. Answer A is not the best answer because it might not have the newest drivers either. Answer C is incorrect because the edition has no effect on how a driver is loaded. Answer D is incorrect because it is always recommended to load only signed drivers whenever possible.
12. Answer **C** is correct because, by default, Internet Explorer blocks most pop-up windows. To allow these sites to work properly, you need to open the Pop-up Blocker Settings dialog box and add the URL of the website to the Allowed sites list to allow pop-ups to be displayed from a specific website. Answer A is incorrect because if the site has been blocked by the network administrator, you usually get a message saying that is the case. Answer B is incorrect because you get a message similar to site not found or site not available. Answer D is incorrect because when a site is not on your trusted list, it typically stops certain programs, such as ActiveX, from running.
13. Answers **A**, **B**, and **C** are correct. As you run out of disk space, your computer cannot swap information using the paging file and cannot create temporary files such as those that are needed when you move files from one drive to another. Your machine also becomes less reliable. Answer D is incorrect because although NTFS supports compression, it does not automatically start compressing files because it is low on disk space.

14. Answer **B** is correct because the Restore advanced settings button on the Advanced tab of the Internet Options dialog box does not affect the other security and privacy setting used by Internet Explorer. Answer A does not change settings if you reinstall Internet Explorer, and this is not an option because Internet Explorer is not part of the OS. Answer C is incorrect because there is no need to use the Reset button on the Advanced tab of the Internet Options dialog box because it results in all of the Internet Explorer settings being reset. Answer D is incorrect because there is no need to reset the zone settings on the Security tab; doing so affects the security level in Internet Explorer, which is not the problem.
15. Answers **A** and **B** are correct because you can shut off the prompts for an individual user account or by using group policies. Answers C and D are incorrect because prompts generated by User Account Control cannot be controlled using the Computer Management console or by using the System Properties.
16. Answer **C** is the correct answer because it is the easiest to implement. Answer A is a possible answer, but it takes much more work to perform. Answer B is not correct because although you could copy wireless settings to the shared folder, the laptop computers would not be able to access them until the wireless network is configured on each laptop. Answer D is incorrect because there is no Autodetect feature that detects a wireless network found on most corporations because of security settings. Answer E is incorrect because there is no group policy that configures wireless settings and the laptops have to be connected to the network to get those settings.
17. Answer **B** is correct. When the boot files become corrupted, you can boot with the Windows 7 installation disk and run the Startup Repair Tool. Answer A is incorrect because Safe mode is used to isolate a bad or corrupt driver or service by loading only the minimum drivers and services for Windows to function. Answer C is incorrect because Safe mode is not started from the Windows 7 installation disc. Answer D is incorrect because you already know that the boot files are corrupted. Therefore, you can repair them by running the Startup Repair Tool.
18. Answer **B** is correct because the Event Viewer shows the logs. Answers A, C, and D are incorrect because none of these utilities exist.
19. Answer **C** is correct because it does not fall in the range of private addresses. Answers A, B, and D are incorrect because they are private addresses. The private addresses are 10.x.x.x, 172.16.x.x to 172.31.x.x, and 192.168.0.x and 192.168.255.x.
20. Answer **C** is correct because BitLocker is the only choice that protects the entire volume. Answers A, B, and D are incorrect because they do not protect everything on the volume.
21. Answer **B** is correct because Task Manager shows processor and memory utilization of all processes. Answer A is incorrect because the Event Viewer shows you the logs. Answer C is incorrect because the Computer Management console is for configuring the system. Answer D is incorrect because the Windows Defender is used to protect against spyware.

22. Answer **D** is correct because `sysprep` removes the SID from the image and cleans up various user and machine settings and log files. Answer A is incorrect because `imagex` is a command-line tool that captures, modifies, and applies installation images for deployment in a manufacturing or corporate environment. Answer B is incorrect because Windows Setup (`setup.exe`) installs the Windows 7 operating system. Answer C is incorrect because `diskpart` is a command-line hard disk configuration utility.
23. Answer **B** is correct because a down arrow means that the device is disabled. Answer A is incorrect because the exclamation point indicates a device that is having a problem. Answers C and D are not indicated in the Device Manager.
24. Answer **C** is correct because the `ping` command is used to test network connectivity. Answer A is incorrect because `ipconfig` is used to show IP addresses of a system. Answer B is incorrect because the `arp` command is used to show the ARP cache. Answer D is incorrect because the `nslookup` command is used to look at and resolve DNS problems.
25. Answer **C** is correct because you will not find Pointer Devices in the Windows Mobility Center. Answers A, B, and D are incorrect because you will find Brightness, Battery Status, and Presentation Settings in the Windows Mobility Center.
26. Answer **A** is correct because an answer file is an XML file that scripts the answers for a series of GUI dialog boxes and other configuration settings used to install Windows. Answer C is incorrect because a Windows image is a copy of a disk volume saved as file. Answer D is incorrect because a catalog is a binary file (.clg) that contains the state of the settings and packages in a Windows image. Answer B is incorrect because it is a made-up answer.
27. Answer **B** is the correct answer because the User State Migration Tool (USMT) is used to migrate the files and settings to a removable media or to a network share and later restore the files and settings to the target computer. Answer A is incorrect because the Windows Easy Transfer (WET) does not use removable media or work over the network; use WET to perform a side-by-side migration to migrate the settings to a new computer that is already running Windows 7. Answer C is incorrect because Windows PE is a bootable tool that replaces MS-DOS as the pre-installation environment. Answer D is incorrect because Sysprep is a utility that facilitates image creation for deployment to multiple destination computers.
28. Answer **A** is correct because the Windows 7 Upgrade Advisor is a utility that enables one to access an easy-to-understand report after scanning your computer. This report specifies whether the currently installed hardware works with Windows 7. Answer B is incorrect because there is no Microsoft utility called System Checker for Windows 7. Answer C is incorrect because System Information gives you a quick view of what components and software your computer has; it does not specify which components do not meet Windows 7 minimum requirements. Answer D is incorrect because the Computer Management console is used to manage the computer.
29. Answer **B** is correct because volumes are managed using the Computer Management console, which is found in administrative tools. Answers A, C, and D are incorrect because these do not exist.

- 30.** Answer **A** is correct because this warning is generated by User Account Control to protect you from an application that might be performing functions that it should not be performing. Answer B is incorrect because this problem has nothing to do with NTFS permissions. Answers C and D are incorrect because this application is asking you to continue, which means you are already running the application as administrator.
- 31.** Answer **B** is correct because Windows Firewall with Advanced Security is used to manage your IPsec configuration because the firewall rules and IPsec settings might conflict with each other. Answers A, C, D, and E are incorrect because the console does none of these.
- 32.** Answer **A** is correct because the Protected Mode prevents COM objects, such as ActiveX controls, from automatically modifying files and settings. With Protected Mode enabled, only users can initiate these types of requests. Answers B, C, and D are incorrect because Protected Mode does not do any of these.
- 33.** Answer **A** is correct because `chkdsk` is used in Windows 7. Answer B is incorrect because the `/F` parameter fixes those errors. Answers C and D are incorrect because `scandisk` was used by the Windows 9X versions of Windows. Answer E is incorrect because it is not Error-Checking, which is accessed from the disk properties.
- 34.** Answers **A** and **B** are correct because Windows ReadyBoost boosts system performance by using USB flash devices as additional sources for caching and Windows ReadyDrive boosts system performance on mobile computers equipped with hybrid drives. Answers C and D state the opposite, so they are incorrect.
- 35.** Answer **A** is the correct answer because if you load the basic VGA driver instead of the new driver, you can then roll back to the previous driver. Answer B is incorrect because you cannot roll back the driver using the command prompt. Answer C is not correct because you cannot roll back the driver, and you don't want to reinstall Windows. Answer D is incorrect because you cannot connect to the update site until you can boot to Windows.
- 36.** Answer **D** is correct because `msconfig` enables you to temporarily disable each program one by one to see which one is causing the problem. Answer A is only available when the computer is not part of the domain and is a clumsy way of performing the same tasks. Answers B and C are incorrect because they are clumsy ways to do it as well.
- 37.** Answers **A** and **B** are correct because Personal mode provides authentication via a preshared key or password and Enterprise mode provides authentication using IEEE 802.1X and EAP. Answers C and D are incorrect because they state the opposite.
- 38.** Answer **B** is correct because you need to flush the DNS cache so that it can get the new address from the DNS server. Answer A is incorrect because it only registers your computer's IP address with the DNS server. Answer C clears the cache, but it is not the most efficient way. Answer D does not correct the problem because the address is still cached.

39. Answer **C** is correct. For a user to access a Windows 7 machine using Remote Desktop, he must be added to the Remote Desktop Users group. Users must also have passwords. Answer A does work but would most likely be a security problem. Answer B is incorrect because the power users group is for backward compatibility. Answer D is incorrect because there is no Telnet group that comes with Windows.
40. Answer **A** is correct because you start the computer and enter the recovery password in the BitLocker Driver Encryption Recovery console. Answer B is incorrect because you did not save the password to disc. Answer C is incorrect because you cannot enter the TPM management console. Answer D is incorrect because you cannot access the BitLocker Driver Encryption Recovery console using the Windows 7 installation disc.
41. Answer **B** is correct because `nslookup` is used to diagnose your DNS infrastructure. Answer A is incorrect because there is no `/dns` option with the `ipconfig` command. Answer C is incorrect because `NBTstat` is used to troubleshoot NetBIOS name resolution problems. Answer D is incorrect because there is no `resolve` command that comes with Windows.
42. Answers **A**, **B**, and **C** are correct because NTFS permissions include Write permission combined with Read and Execute. The Contributor share permission gives the ability read, write, execute, and delete. When you combine the two, you take the least, so that would be read, write, and execute. Answer D is incorrect because there was no delete NTFS permission given. Because Pat has permissions, Answer E is incorrect.
43. Answer **A** is correct because Windows PE is short for Microsoft Windows Pre-installation Environment. It is a bootable tool that replaces MS-DOS as the pre-installation environment. Windows PE is not a general purpose operating system. Instead it is used to provide operating system features for installation, troubleshooting, and recovery. Answer C is incorrect because a Windows image is a copy of a disk volume saved as file. Answer D is incorrect because a catalog is a binary file (.clg) that contains the state of the settings and packages in a Windows image. Answer B is incorrect because it is a fictional answer.
44. Answer **C** is correct because the name of the answer file is `autoattend.xml`. Answers A, B, and D are incorrect because they are fictional answers.
45. Answer **B** is correct because an intranet is defined as part of the organization's network that does not require a proxy server. Answer A is incorrect because it defines this as the Internet zone. Answer C is incorrect because this describes the trusted zone. Answer D is incorrect because this defines the restricted zone.
46. Answer **C** is correct because you need to have a pop-up blocker to stop the windows from opening. Answers A and B are incorrect because they do not stop the pop-up windows. Answer D is incorrect because Windows Defender is designed to primarily protect against spyware; however, Windows Defender helps a little against some pop-ups that are generated by spyware programs.

- 47.** Answer **B** is correct because the Trusted Platform Module (TPM) is a special microchip that supports advanced security features. Answer A is incorrect because ActiveX includes special controls used in Internet Explorer plug-ins. Answer C is incorrect because Dynamic Protection is used to make sure web applications cannot access files on the computer. Answer D is incorrect because NTFS is a file system.
- 48.** Answer **C** is correct because EFS, which is short for Encrypted File System, is used to encrypt individual files. Answer A is incorrect because NTFS is the secure file system used in Windows 7 that support both compression and EFS. Answer B is incorrect because compression is used to compress files, not encrypt them. Answer D is incorrect because BitLocker is used to encrypt entire disk volumes.
- 49.** Answer **C** is correct because the file the memory content is saved during hibernation is hiberfil.sys. Answer A is a fictional file. Answer B is the name of the paging file used in Windows XP, Vista, and 7. Answer D is incorrect because power.sys is a system file used in Windows to help manage power settings.
- 50.** Answer **A** is correct. When you want to configure event subscriptions, you run the `winrm quickconfig` command on all source computers and run the `wecutil qc` command (Answer B) on the target computer. You must also add the computer account of the target computer to the local Administrators group of the source computer. Answers C and D are incorrect because there is no `tether` or `subscribe` command available.

# Index

## Numerics

---

64-bit processors, 30

802.1X, 226

## A

---

accelerators, 467-469

accessibility, configuring, 116-118

accessing System Recovery Options  
menu, 551-552

ACE (access control entry), 321

ACLs (access control lists), 321

ACT (Application Compatibility  
Toolkit), Compatibility Administrator,  
426

Action Center, 542

activating Windows 7, 70

active partitions, 162

ActiveX controls, deleting, 454

ActiveX Opt-in (IE 8.0), 459

ad hoc wireless adapters, 225

add-ons (IE 8.0)

disabling, 453

displaying, 452

adding

computers to domain, 112

devices, 129

passwords to Windows vault, 295

address classes (IPv4), 196-197

Administrative Tools, 146

MMC, 145

using on remote computers, 502

administrator account, 286

Advanced Boot Options menu,  
546-548

advanced file sharing, enabling,  
373-374



**Aero, 50-52, 136**

**AIK (Automated Installation Kit),  
deploying Windows 7, 84**

**AIS (Application Information Service),  
299**

**analog modems, 238**

**answers to practice exam, 584-590**

**anycast addresses, 200**

**applications**

compatibility settings, configuring,  
423-426

default programs, 114

software restrictions, 432-437

Start menu, 39-40

uninstalling, 113

Windows Live Essentials, 420-421

**AppLocker, 433-437**

**assigning NTFS permissions, 325**

**associated programs, changing for  
filename extensions, 114**

**auditing, 310**

policies, creating, 311-312

printer access, 409-410

**authentication, 282**

permissions, 284

UAC, 299-300

enabling/disabling for user  
accounts, 301, 304

message behavior, changing,  
305-306

policy settings, 304

**authentication rules, configuring, 273**

**AutoComplete settings (IE 8.0),  
configuring, 451**

## **B**

---

**backing up BCD, 73**

**Backup and Restore Center, 562**

**backups, 559-560**

full backups, tape rotation, 561

restore points, 564-567

Shadow Copy, 566

System Image Backup, 564

**base scores (WEI), 523-524**

**basic disks, 163**

converting from dynamic disks, 166

converting to dynamic disks, 164-166

managing, 163-164

**battery power levels, configuring for  
mobile computers, 485-486**

**BCD, 71-73**

**bcdedit, 72, 75**

command options, 74-75

**bcdedit, 71**

**BIOS (Basic Input/Output System),  
161**

**BitLocker Drive Encryption, 343, 348**

system requirements, 350

TPM security hardware, 349-351

turning off, 352

turning on, 351

**BitLocker To Go, 352-354**

**Bluetooth, connecting mobile devices,  
491**

**boot loader, 71**

**boot partitions, 162**

**boot tools**

Advanced Boot Options menu, 546-  
548

System Configuration, 549-550

**bootup**

system repair discs, creating, 552-553

VHD images, 96-101

**BrancheCache, configuring, 383-385**

**breaking mirrored volumes, 178**

**broadband connections, remote  
access, 241-242**

**browse libraries, 332**

**browsing history, configuring, 450**

**C****certificate mapping, 283****certificates, 463-464**

encryption, 345-347

viewing, 458

**changing NTFS permissions, 323-324****CHAP (Challenge Handshake Authentication Protocol), 243****Check Disk, 183-184, 187****chkntfs command, 184****clean Windows 7 installation, 63****cmdlets, 506****color and appearance of desktop, changing, 137****color depth, setting, 138****commands, PowerShell, 507****comparing**

64- and 32-bit processors, 30

local and network printers, 394-395

**compatibility**

settings, configuring, 423-426

Windows Aero, troubleshooting, 143

Windows XP Mode, 427-429

**Compatibility Administrator (ACT), 426****Compatibility View (IE 8.0), 467****compression**

NTFS, 356

zipped folders, 355

**computer name, changing, 112****configuring**

accessibility, 116-118

AppLocker rules, 434-437

authentication rules, 273

BranchCache, 383-385

compatibility settings, 423-426

connection security rules, 272-275

display settings

color and appearance, 137

color depth, 138

Ease of Access Center, 139-140

multiple monitor configuration, 140

resolution, 137

themes, 136

**IE 8.0**

AutoComplete settings, 451

browsing history, 450

content zones, 456-457

security settings, 454-455, 458-464

IP addressing on Windows 7, 205-207, 210-211

keyboard, 129

mobile computers

battery power levels, 485-486

power plans, 481, 484

presentation settings, 478-481

shutdown options, 484-485

mouse, 129

policies, group policies, 148

printers, 401-402

location-aware printing, 403

permissions, 404-405

print jobs, 407-408

print spooler, 405-407

processor scheduling, 527

remote projectors, 493-494

services, 146

sound, 130-131

synchronization, 486-487

offline folders, 488, 491

sync partnerships, 491-492

virtual memory, 526-527

Windows Defender, 261-262

Windows Firewall, 266-269

Windows SideShow, 492

wireless networks, 227-232

**connecting**

mobile devices, 491

to remote computers

Remote Desktop, 498-500

## connecting

- requirements, 498
- to shared folders, 379-382

**connection security rules, configuring, 272-275**

**connectivity**

- printers, troubleshooting, 410-411
- troubleshooting, 212-217

**content zones, 456-457**

**Control Panel, 109, 477**

- Device Manager, 127-129
- power plans, configuring for mobile computers, 481, 484
- system information, viewing, 111
- views, 110

**controlling access to USB flash devices, 327-328**

**converting**

- basic disks to dynamic disks, 164-166
- dynamic disks back to basic disks, 166

**cookies, 454-455**

**copy backups, 561**

**copying files, NTFS, 326**

**creating**

- auditing policies, 311-312
- Homegroups, 377-379
- local user accounts, 290-293
- passwords, 293-294
- system images, 564
- system repair discs, 552-553

**Credentials Manager, adding passwords, 295**

**Cross-Domain Barriers, 459**

**customizing**

- Notification Area, 42
- taskbar, 47-49

## D

**data synchronization**

- configuring, 486, 488
- offline folders, configuring, 488, 491

- sync partnerships, configuring, 491-492

**DCS (Data Collector Sets), 520-521**

**decrypting EFS (encrypting file system), 345**

**default gateway, 197, 202**

**default programs, 114**

**default settings, restoring on IE 8.0, 466-467**

**default user accounts, 286**

**defragmenting hard drives, 184-185**

**deleting ActiveX controls, 454**

**deploying Windows 7, 84**

- AIK, 84
- DISM, 91, 93
- WDS, 94-95
- Windows PE, 84-85

**desktop, 35**

- icons
  - adding/removing, 36
  - hiding, 37
- shortcut, adding, 36
- themes, changing, 136

**device drivers, 123-125**

**Device Manager, 127-129**

**devices**

- adding, 129
- mobile devices, connecting, 491
- plug and play, 124

**Devices and Printers folder, 125-127**

**DHCP (Dynamic Host Configuration Protocol), 204**

**diagnostic tools**

- Memory Diagnostics, 545
- Network Diagnostics, 546

**dial-up connections, remote access, 237-240**

**differential backups, 560**

**DirectAccess, 246-248**

**disabling IE 8.0 add-ons, 453**

**disk caching, ReadyBoost, 528-529**

**Disk Defragmenter, 185**

**Disk Management console, 158**

**disk management tools**

- Disk Management console, 158
- disk storage management, 162
  - basic disks, 163
  - converting basic disks to dynamic disks, 164-166
  - converting dynamic disks back to basic disks, 166
  - dynamic disks, 163
  - managing basic and dynamic disks, 163-164
- Diskpart, 159-161
- file systems, 167-168
- partitioning, 161-162

**disk partitioning, 161-162**

**disk storage management, 162**

- basic disks, 163
- converting basic disks to dynamic disks, 164-166
- converting dynamic disks back to basic disks, 166
- dynamic disks, 163
- managing basic and dynamic disks, 163-164

**Diskpart, 158-161**

**DISM (Deployment Image Servicing and Management), 91-93**

**display settings**

- color and appearance, changing, 137
- color depth, configuring, 138
- Ease of Access Center, configuring, 139-140
- multiple monitors, configuring, 140
- resolution, configuring, 137
- themes, changing, 136
- Windows Aero, 141-143

**displaying**

- IE 8.0 add-ons, 452
- wireless connection characteristics, 228

**DNS (Domain Naming System), name resolution, 203-204**

**domain user accounts, 285**

**domains, 284**

- adding/removing computers from, 112
- wireless networks, 233

**downloading**

- Windows Live Essentials, 421
- Windows Virtual PC, 428

**drivers**

- print drivers, 395
- signed drivers, 124-125

**dual-boot system, enabling, 75-77**

**dynamic disks, 158**

- converting back to basic disks, 166
- converting from basic disks, 164-166
- managing, 163-164

**dynamic security (IE 8.0), 458-459**

---

**E**

**EAP (Extensible Authentication Protocol), 243**

**Ease of Access Center**

- accessibility, configuring, 116-118
- display settings, configuring, 139-140

**editions of Windows 7, 29**

**EFI (Extensible Firmware Interface), 161**

**EFS (encrypting file system), 343-345**

- encryption certificates, 345-347
- recovery agents, 347-348

**enabling**

- dual-boot system, 75-77
- features, 113
- file sharing, 371-374
- frame transparency, 136
- network discovery, 366-368
- Parental Controls, 118-119
- Remote Assistance, 502

**encryption, 342**

BitLocker Drive Encryption,  
348-350

TPM security hardware, 351

turning off, 352

turning on, 351

BitLocker To Go, 352-354

EFS, 343-345

encryption certificates, 345-347

recovery agents, 347-348

**Error-checking tool, 183****establishing remote PowerShell sessions, 508****Event Viewer, 537-539****events**

filtering, 540

levels of, 539

subscriptions, 541

**exam, practice exam, 573-583**

answers, 584-590

**exFAT (Extended File Allocation Table), 168****extended display settings, configuring, 140****extending simple or spanned volumes, 173-174****Extensible Authentication Protocol. See EAP****F**

---

**FAT (file allocation table), 167****FAT16, 167****FAT32, 167****features**

of IE 8.0, 447-448

turning on, 113

**file sharing**

advanced sharing, enabling, 373-374

BranchCache, configuring, 383-385

enabling, 371

**file structure (Windows 7), 329-330**

folder options, 334-335

libraries, 331-333

**file synchronization, configuring, 486-491****file systems, 167-168****filename extensions, changing associated programs, 114****files**

copying (NTFS), 326

moving to desktop, 36

owners (NTFS), 326-327

**filtering events, 540****firewalls**

Windows Firewall, 264-269

Windows Firewall with Advanced Security, 269-272

**flash devices, disk caching with ReadyBoost, 528-529****flash RAM, ReadyDrive, 529****folders**

Administrative Tools, 145-146

Devices and Printers folder, 125-127

owners, NTFS, 326-327

shared folders, 375

connecting to, 379-382

creating, 374

managing, 379

offline folder synchronization,  
488, 491

Windows 7, 330, 334-335

**format command, 180****formatting disk volumes, 180-181****FQDNs (fully qualified domain names), 202****fragmentation, reducing, 185****full backups, 560-561****G**

---

**gadgets, 49-50****GFS (Grandfather, Father, Son) backup rotation, 561****global unicast addresses, 199**

**GPOs (Group Policy Objects), 148**

**GPT (GUID partition table), 161**

**group policies, configuring, 148**

**guest accounts, 286**

## H

---

### hard disk drives

defragmenting, 184-185

formatting, volumes, 180-181

optimizing, 182

    monitoring disk space, 183

    NTFS disk quotas, 185-187

    running Check Disk, 183-184

**hiding icons on desktop, 37**

**home networks, wireless connections, 233**

**Homegroups, 375-379**

**hybrid drives, ReadyDrive, 529**

**hybrid sleep, 484**

**hypervisor, 97**

## I

---

**IA-32 processor, 31**

### icons

adding/removing from desktop, 36

hiding on desktop, 37

rearranging on taskbar, 48

**IE (Internet Explorer) 8.0, 446**

accelerators, 467, 469

add-ons

    disabling, 453

    displaying, 452

AutoComplete settings, configuring, 451

browsing history, configuring, 450

certificates, viewing, 458

Compatibility View mode, 467

features, 447-448

Internet Options dialog box, 450

messages, 461

RSS feeds, subscribing to, 465-466

search providers, adding, 469

security

    certificates, 463-464

    content zones, 456-457

    cookies and privacy settings, 454-455

    dynamic security, 458-459

    InPrivate Browsing, 461-463

    Parental Controls, 463

    protected mode, 461

web pages, saving, 465

**IKEv2 (Internet Key Exchange), 243**

### images

DISM, 91-93

VHD image, booting with, 96-101

**incremental backups, 560**

**indexes, improving searches, 339-341**

**Information Bar (IE 8.0), messages, 461**

**infrastructure wireless adapters, 225**

**InPrivate Browsing (IE 8.0), 461-463**

### installing

printers

    local printers, 396, 400

    network printers, 401

recovery certificates, 348

updates, 68-70

Windows 7, 60

    clean installation, 63

    memory requirements, 61

    minimum hardware requirements, 61

    System Preparation Tool), 85-87

    unattended installation, 87

    WDS, 94-95

    WIM files, 88-91

    Windows SIM, 87-88

Windows Virtual PC, 428

Windows XP Mode, 428-429

**Instant Search List (IE 8.0), adding search providers, 469**

**Internet Explorer Compatibility Test Tool (ACT), 427**

**Internet Explorer Zoom, 448**

**Internet Key Exchange (IKEv2), 243**

**Internet Options dialog box (IE 8.0), 450**

**Internet zones, 456**

**IP addressing**

address classes, 196-197

default gateway, 197, 202

DHCP, 204

IPv6, 198-200

name resolution, 202-204

netsh command, 210-211

Windows 7, configuring, 205-207

**IPsec, 242, 272-275**

**IPv4, 196, 201**

**IPv6, 198-200**

## J-K

---

**Jump Lists, 44**

**Kerberos authentication, 283**

**keyboard, configuring, 129**

**keys (Registry), 149**

## L

---

**L2TP (Layer 2 Tunneling Protocol), 242**

**LANs (local area networks), 226**

**laptops. See mobile computers, configuring**

**LDR (Logical Disk Manager), 163**

**levels of events, 539**

**libraries**

browse, 332

search-only, 332

Windows 7, 331-333

**link-local addresses, 199**

**LLTD (Link Layer Topology Discovery), 366**

**LoadState command (USMT), 80**

**Local Group Policy Editor, opening, 148**

**local intranet zones, 456**

**local printers, 394**

drivers, 395

installing, 396, 400

**local user accounts, 285-287**

creating, 290-293

logon names, 288

managing, 289, 292-294

passwords, 288-289

removing, 293

**location-aware printing, configuring, 403**

**locations of wireless networks, 233-235**

**logon names, 288**

## M

---

**magnifying web pages, 448**

**managing**

basic and dynamic disks, 163-164

images with DISM, 91-93

local logon accounts, 289, 292-294

NTFS permissions, 324

print spooler, 405-407

shared folders, 379

**Master Boot Record (MBR), 161**

**maximizing windows, 47**

**MBR (Master Boot Record), 161**

**memory**

SuperFetch, 527

usage, 524-526

virtual memory, configuring, 526-527

**Memory Diagnostics, 545**

**message behavior (UAC), changing, 305-306**

**messages, IE 8.0, 461**

**Microsoft CHAP version 2 (MS-CHAP v2), 243**

**minimum hardware requirements,**  
**Windows 7 installation, 61**

**mirrored volumes, 176-179**

**MMC (Microsoft Management Console), 145**

remote management, 502

**mobile computers, configuring**

battery power levels, 485-486

power plans, 481, 484

presentation settings, 478-481

shutdown options, 484-485

sync partnerships, 491-492

synchronization, 486-488, 491

**Mobility Center, 477**

opening, 478

presentation settings, configuring,  
 478-481

**modems, analog, 238**

**monitoring**

disk space, 183

events

Event Viewer, 537-541

Reliability Monitor, 541-542

system performance

memory usage, 524-526

Performance Monitor, 521

Resource Monitor, 519

Task Manager, 517-519

**monitors, configuring Windows SideShow, 492**

**mount points, volumes, 179**

**mouse, configuring, 129**

**moving files (NTFS), 326**

**MS-CHAP v2 (Microsoft CHAP version 2), 243**

**msinfo32.exe, 543**

**multi-boot configuration, 167**

**multicast addresses, 200**

**multiple monitors, configuring, 140**

## **N**

---

**name resolution, 202-204**

**need-to-know security, 298**

**NetBIOS, 365**

**netsh command, configuring IP addressing, 210-211**

**Network and Sharing Center, 208**

**network connectivity, troubleshooting, 212-217**

**Network Diagnostic tool, 546**

**network discovery, enabling, 366-368**

**network printers, 394**

drivers, 395

installing, 401

print jobs, configuring, 407-408

**network projectors, configuring, 493-494**

**networks**

remote access, 236

broadband connections, 241-242

dial-up connections, 237-240

DirectAccess, 246-248

VPNs, 242-246

wireless. *See* wireless networks

**normal backups, 560**

**Notification Area, 42-43**

**NTFS, 167, 320-321**

compression, 356

controlling access to USB flash devices, 327-328

copying and moving files, 326

disk quotas, 185-187

folder and file owners, 326-327

permissions, 321

assigning, 325

managing, 324

setting, viewing, changing or removing, 323-324

special permissions, 322

viewing, 324

**NTLM (Windows NT LAN Manager), 283**



opening

## O

---

### opening

- Local Group Policy Editor, 148
- Mobility Center, 478
- System Recovery Options menu, 551-552

### optimizing

- boot speed, 551
- disks, 182
  - defragmenting hard drives, 184-185
  - monitoring disk space, 183
  - NTFS disk quotas, 185-187
  - running Check Disk, 183-184

## P

---

**packet filters, 265**

**paging, 521**

**paging file, 521, 524-527**

**PAP (Password Authentication Protocol), 243**

**Parental Controls, enabling, 118-119**

**Parental Controls (IE 8.0), 463**

**partition tables, basic disks, 163**

**partitions, 161-162**

**passwords, 288-289**

- adding to Windows vaults, 295
- creating, 293-294

### performance

- disk caching, ReadyBoost, 528-529
- memory
  - SuperFetch, 527
  - usage, 524-526
- processor scheduling, configuring, 527
- system performance, monitoring, 517-521
- WEI, 522-524

**Performance Monitor, 521**

**permissions, 284**

- NTFS, 321

- assigning, 325

- managing, 324

- setting, viewing, changing, or removing, 323-324

- special permissions, 322

- viewing, 324

- printer permissions, configuring, 404-405

**pinning items to Start menu, 45**

**pinning items to taskbar, 44**

**plug and play devices, 124**

### policies

- Audit Object Access policy, auditing printer access, 409-410

- creating, 311-312

- GPOs, 148

- software restriction policies, 432-437

**policy settings (UAC), 304**

**power plans, configuring on mobile computers, 481, 484**

**PowerShell, 505**

- cmdlets, 506

- commands, 507

- remote sessions, creating, 508

**PPP (Point-to-Point Protocol), 226**

**PPPoE (Point-to-Point Protocol over Ethernet), 242**

**PPTP (Point-to-Point Tunneling Protocol), 242**

**practice exam, 573-583**

- answers, 584-590

**presentation settings, configuring on mobile computers, 478-481**

**print devices, 393**

**print drivers, 393**

**print jobs, configuring, 407-408**

**print spooler, managing, 405, 407**

**printers, 393**

- access, auditing, 409-410

- configuring, 401-402

- connectivity, troubleshooting, 410-411

- local printers, 394
  - drivers, 395
  - installing, 396, 400
- location-aware printing, configuring, 403
- network printers, 394
  - drivers, 395
  - installing, 401
  - permissions, configuring, 404-405
- printing process, 395-396**
- privacy settings, IE 8.0, 454-455**
- Problem Steps Recorder, 554-555**
- processor scheduling, configuring, 527**
- processors, 64-bit, 30**
- Program Compatibility Troubleshooting, configuring compatibility settings, 423-424**
- programs**
  - device drivers, 123
  - uninstalling, 113
- protected mode (IE 8.0), 461**
- protecting against spyware, 258-260**
- Public folders, sharing, 369-370**
- public networks, wireless connections, 233**

## **Q-R**

---

- RAM, monitoring utilization, 521**
- ReadyBoost, 528-529**
- ReadyDrive, 529**
- rearranging icons on taskbar, 48**
- recording steps, 554**
- recovery agents, encryption, 347-348**
- recovery certificates, installing, 348**
- reducing fragmentation, 185**
- reg files, 150**
- Registry**
  - keys, 149
  - values, 150
- Registry Editor, 149**
- reliability, 535**
- Reliability Monitor, 541-542**
- remote access, 236-237**
  - broadband connections, 241-242
  - dial-up connections, 237-240
  - DirectAccess, 246-248
  - VPNs, 242-246
- Remote Assistance, 501-502**
- remote computers, connecting to**
  - Administrative Tools, 502
  - Remote Desktop, 498-500
  - requirements, 498
- Remote Desktop, 497-500**
- remote management, establishing PowerShell sessions, 508**
- remote projectors, configuring, 493-494**
- removing**
  - computers from domain, 112
  - local user accounts, 293
  - mirrored volumes, 178
  - mount-point folder paths, 179
  - NTFS permissions, 323-324
  - restore points, 567
- requirements**
  - for remote computer connections, 498
  - for Windows Aero, 141
- resetting IE 8.0 settings, 466-467**
- resolution, setting, 137**
- Resource Monitor, monitoring system performance, 519**
- restore points, 564-567**
- restoring**
  - IE 8.0 default settings, 466-467
  - to previous version of Windows, 70
- restricted sites zones, 456**
- restricting software, 432-437**
- RSS feeds, subscribing to, 465-466**
- rules (AppLocker), configuring, 434-437**
- running Check Disk, 183-184**

## S

---

**Safe Mode, 546**

**saving web pages, 465**

**Scandisk, 158**

**ScanState command (USMT), 80**

**scripting, PowerShell, 505**

cmdlets, 506

commands, 507

remote sessions, creating, 508

**search box (Start menu), 338**

**search providers, adding to IE 8.0, 469**

**search-only libraries, 332**

**searching in Windows 7, 336**

improving with index, 339-341

search tools, 337-339

**Secure Socket Tunneling Protocol.**

**See SSTP**

**security**

auditing, 310-312

authentication, 282-284

IE 8.0

certificates, 463-464

content zones, 456-457

cookies and privacy settings, 454-455

dynamic security, 458-459

InPrivate Browsing, 461-463

messages, 460-461

Parental Controls, 463

protected mode, 461

IPsec, 272-275

need-to-know, 298

Parental Controls, enabling, 118-119

permissions (printer), configuring, 404-405

software restriction policies, 432-437

UAC, 299-300

enabling/disabling, 301, 304

message behavior, changing, 305-306

policy settings, 304

Windows Firewall, 264-269

Windows Firewall with Advanced Security, 269-272

Windows XP, 25

wireless connections, 230

**select command, 159**

**services, configuring, 146**

**Setup Analysis Tool (ACT), 427**

**Shadow Copy, 566**

**shared folders, 375**

connecting to, 379-382

creating, 374

managing, 379

offline folder synchronization, 488, 491

**sharing**

Homegroups, 375-379

Public folders, 369-370

**shortcuts, adding to desktop, 36**

**shrinking volumes, 174**

**shutdown options, configuring for mobile computers, 484-485**

**SIDs (security IDs), 288**

**signed drivers, 124-125**

**simple volumes, 171-174**

**slideshows, configuring remote projectors, 493-494**

**SMB (server message block), 365**

**software restrictions, 432-437**

**sound, configuring, 130-131**

**spanned volumes, 172-174**

**split tunneling, VPNs, 245-246**

**spooler, 393**

**spyware**

protecting against with Windows Defender, 258-260

Windows Defender, 256-258

**SSD (solid state drives), 481**

**SSL (Secure Sockets Layer), 463**

**SSTP (Secure Socket Tunneling Protocol), 243**

**standard equipment, MBR disks, 161**

**Standard User Analyzer (ACT), 427****Start menu, 38, 41**

- applications, 39-40
- pinning items to, 45
- search box, 338

**startup**

- Advanced Boot Options menu, 546-548
- boot speed, optimizing, 551
- System Configuration tool, 549-550
- system repair discs, creating, 552-553

**storage, disk storage management, 162**

- basic disks, 163
- disks, converting, 164-166
- dynamic disks, 163-164

**striped volumes, 174-176, 181****subscribing to RSS feeds, 465-466****subscriptions (events), 541****SuperFetch, 527****Sync Center, configuring synchronization, 486-488, 491****sync partnerships, configuring, 491-492****synchronization**

- configuring, 486-488
- offline folders, configuring, 488, 491

**Sysprep (System Preparation Tool), installing Windows 7, 85-87****System Configuration tool, 549-550****system health, viewing with Reliability Monitor, 541-542****System Image Backup, 564****System Information, 111, 543****system partition/volume, 162****system performance**

- disk caching, ReadyBoost, 528-529
- memory usage, monitoring, 524-526
- monitoring tools
  - Performance Monitor, 521
  - Resource Monitor, 519
  - Task Manager, 517-519

- processor scheduling, configuring, 527

**System Recovery Options menu, accessing, 551-552****system repair discs, creating, 552-553****system requirements, BitLocker Drive Encryption, 350****System Restore, 564-567****T****tape rotation, 561**

- GFS backup rotation, 561

**Task Manager, 517-519****taskbar, 37**

- customizing, 47-49
- icons, rearranging, 48
- Notification Area, 42-43
- pinning items to, 44

**TCP/IP**

- IP addressing, 196
  - address classes, 196-197
  - default gateway, 197, 202
  - DHCP, 204
  - name resolution, 202-204
  - netsh command, 210-211
  - Windows 7, configuring, 205-207
- IPv6, 198-200

**themes, enabling frame transparency, 136****tools**

- disk management tools, 158
  - Disk Management console, 158
  - disk storage management, 162-166
  - Diskpart, 159-161
  - file systems, 167-168
  - partitioning, 161-162
  - Windows search tools, 337-339

**TPM (Trusted Platform Module), 349-351****troubleshooting**

- compatibility issues, 426

## diagnostic tools

Memory Diagnostics, 545

Network Diagnostic tool, 546

network connectivity, 212-217

printers, 410-411

Problem Steps Recorder, 554-555

## startup

Safe Mode, 547-548

System Configuration tool,  
549-550

upgrades, 67

**trusted sites zones, 456****turning on features, 113****U****UAC (User Account Control), 299-300**enabling/disabling for user accounts,  
301, 304message behavior, changing, 305-306  
policy settings, 304**unattended Windows 7 installation, 87****uninstalling programs, 113****unique local unicast addresses, 200****updates, installing, 68-70****upgrading Windows, 63-67****USB devices, controlling access to,  
327-328****user accounts, 285**

default accounts, 286

local accounts, 286-287

logon names, 288

managing, 289, 292-294

passwords, 288-289

## UAC

enabling/disabling, 301, 304

message behavior, changing,  
305-306

policy settings, 304

**USMT (User State Migration Tool),  
78-80****V****values (Registry), 150****vaults, adding passwords, 295****verifying signed drivers, 125****versions of Windows, 28**

compatibility

configuring, 423-426

Windows XP Mode, 427-429

restoring to previous version, 70

upgrading, 63-67

**VHD images, booting with, 96-101****viewing**

certificates, 458

NTFS permissions, 323-324

Registry, 149

system health with Reliability  
Monitor, 541-542system information in Control Panel,  
111**views, Control Panel, 110****virtual memory**

configuring, 526-527

paging file, 524-526

**volumes, 169-170**extended simple or spanned volumes,  
173-174

formatting disks, 180-181

mirrored volumes, 176-179

mount points, 179

shrinking, 174

simple volumes, 171-172

spanned volumes, 172-173

striped volumes, 174-176, 181

**VPNs (Virtual Private Networks),  
remote access, 242-246****W****WDS (Windows Deployment Services),  
installing Windows 7, 94-95****web browsers, IE 8.0, 446**

accelerators, 467-469

- add-ons, 452-453
  - certificates, viewing, 458
  - Compatibility View, 467
  - default settings, restoring, 466-467
  - features, 447-448
  - Internet Options dialog box, 450
  - RSS feeds, subscribing to, 465-466
  - search providers, adding, 469
  - security settings, 454-464
  - web pages, saving, 465
- web pages**
- saving, 465
  - zooming in/out, 448
- WEI (Windows Experience Index), 522-524**
- Welcome Center, 109**
- WEP (Wireless Equivalent Privacy), 226**
- WET (Windows Easy Transfer), 78**
- WIM files, installing, Windows 7, 88-91**
- windows, maximizing, 47**
- Windows, upgrading, 63-67**
- Windows 7, 26**
- activating, 70
  - deploying
    - AIK, 84
    - Windows PE, 84-85
  - installing, 60
    - clean installation, 63
    - memory requirements, 61
    - minimum hardware requirements, 61
    - Sysprep, 85-87
    - unattended installation, 87
    - WDS, 94-95
    - WIM files, 88-91
    - Windows SIM, 87-88
  - IP addressing, configuring, 205-207
  - popular folders, 330
  - searching, 336
    - improving with index, 339-341
    - search tools, 337-339
  - updating, 68-70
- Windows 7 Enterprise, 29**
- Windows 7 Home Basic, 29**
- Windows 7 Home Premium, 29**
- Windows 7 Professional, 29**
- Windows 7 Starter, 29**
- Windows 7 Ultimate, 30**
- Windows 7 Upgrade Advisor, 66**
- Windows Defender, 256-258**
- configuring, 261-262
  - spyware, protecting against, 258-260
- Windows Explorer, 336**
- Windows Firewall, 264-269**
- Windows Firewall with Advanced Security, 269-272**
- Windows Flip 3D, 50**
- Windows Live Essentials, 420-421**
- Windows PE (Preinstallation Environment), 84-85, 553-554**
- Windows SideShow, configuring, 492**
- Windows Virtual PC, installing, 428**
- Windows Vista, 25, 75-77**
- Windows XP, 25**
- Windows XP Mode, 427-429**
- wireless adapters, 225**
- wireless networks, 224-230**
- configuring, 227-232
  - connections, 233
  - locations, 233-235
  - standards, 225
- workgroups, 284**
- WPA (Wi-Fi Protected Access), 226**
- WPA2 (Wi-Fi Protected Access Version 2), 226**

---

## X-Y-Z

**zooming in/out of web pages, 448**