Covers All Exam Objectives

Includes Real-World Scenarios, Hands-on Exercises, and Leading-Edge Exam Prep Software Featuring

- Custom Testing Engine
- Windows Vista Simulation Software
- Hundreds of Sample Questions
- Electronic Flashcards for PCs, Pocket PCs, and Palm Handhelds
- Entire book in PDF

MCTS

Microsoft® Windows Vista™ Client Configuration STUDY GUIDE

Exam 70-620

Michael Aldridge
Josh Evitt
Lisa Donald
James Chellis

SYBEX SERIOUS SKILLS.

MCTS

Microsoft® Windows Vista™ Client Configuration

Study Guide

MCTS

Microsoft® Windows Vista™ Client Configuration

Study Guide

Michael Aldrigde
Josh Evitt
Lisa Donald
James Chellis

Wiley Publishing, Inc.

Acquisitions Editor: Jeff Kellum
Development Editor: Kim Wimpsett
Technical Editors: Randy Muller and Chris Crayton
Production Editor: Sarah Groff-Palermo
Copy Editor: Liz Welch
Production Manager: Tim Tate
Vice President and Executive Group Publisher: Richard Swadley
Vice President and Executive Publisher: Joseph B. Wikert
Vice President and Publisher: Neil Edde
Media Project Supervisor: Laura Atkinson
Media Development Specialist: Steve Kudirka
Media Quality Assurance: Kate Jenkins
Book Designer: Bill Gibson, Judy Fung
Compositor: Laurie Stewart, Happenstance Type-O-Rama
Proofreader: Rachel Gunn
Indexer: Ted Laux
Anniversary Logo Design: Richard Pacifico
Cover Designer: Ryan Sneed

Published simultaneously in Canada

ISBN-13: 978-0-470-10881-9

10 9 8 7 6 5 4 3 2 1

Sybex®
An Imprint of
WILEY

To Our Valued Readers:

Thank you for looking to Sybex for your Microsoft Windows Vista certification exam prep needs. The Sybex team at Wiley is proud of its reputation for providing certification candidates with the practical knowledge and skills needed to succeed in the highly competitive IT workplace. Just as the Microsoft Learning is committed to establishing measurable standards for certifying individuals who configure Windows Vista operating systems, Sybex is committed to providing those individuals with the skills needed to meet those standards.

The author and editors have worked hard to ensure that the Study Guide you hold in your hands is comprehensive, in-depth, and pedagogically sound. We're confident that this book will exceed the demanding standards of the certification marketplace and help you, the Windows Vista certification candidate, succeed in your endeavors.

As always, your feedback is important to us. If you believe you've identified an error in the book, please visit Wiley's Technical Support web site at `wiley.custhelp.com`. If you have general comments or suggestions, feel free to drop me a line directly at `nedde@wiley.com`. At Sybex we're continually striving to meet the needs of individuals preparing for certification exams.

Good luck in pursuit of your Windows Vista certification!

Neil Edde
Vice President & Publisher
Sybex, an Imprint of Wiley

For Karen. You are the best wife that a man could ask for, the best mother that a child could ask for, and the best friend that anyone could ask for. Beyond death do us part.
—Michael Aldridge

For Tiffany. Your laughter brightens my day, and your love brightens my life. I'm so blessed to be married to my best friend.
—Josh Evitt

Acknowledgments

Certification and teaching are in my blood. Even after getting certifications for the past nine years, the challenge never gets old to me. There's always that next certification to get. It's my goal to pass on that "certification fever" to you, as well as provide knowledge that you can use in your career.

First and foremost, I'd like to thank my Lord and Savior, Jesus Christ. Without Him, I'd have nothing. With Him, I have everything.

My everlasting thanks goes to my wife, Karen, and my sons, Hayden and Brandon. Thank you for being understanding when I had to write during the late nights and weekends. I love you all dearly.

Thanks to my mother and father, who made sure that I had a computer in my hands at age 10. Thanks to my brother and sister, Tim and Tonya, my first "students." And thanks to my sister Anna, whom I enjoy helping when she calls me with homework questions.

Thanks to my friend, business partner, and co-author, Josh Evitt, for his friendship and patience. I wouldn't have wanted to simultaneously tackle a book and a new business with anyone else.

Thanks to Tanner Clayton, for introducing us to James Chellis, and thanks to James for giving us this opportunity. I hope we have exceeded your expectations. A special thanks goes to Will Schmied for encouraging me to write this book.

Thanks to those who have fought in the trenches with me in my IT career, including Alan, Wayne, John, Douglas, Dale, Joe, Charles, Matthew, Rick, Randy, Robert, and Christine. You made working in IT enjoyable.

A big shout-out goes to my certification forums family. Mitzs, thanks for getting me started. Ash, Bags, Becky, BORF, ;De', Fortch, Geek, Jim, Koen, LnR, Mary, Matt/cbt, MM, msChris, N'awlins, ND, P4F, Q, sc0rp, Sean, Snoopy, Squick, supa, Tcat, Tinus, Todd, Tomshawk, Toni, Toss, TMK, Trip, USS, WD, Z0r, and all the countless others (I wish I could list you all) whom I've gotten to know online, thanks for making me feel welcome. Rest in peace, d-Faktor.

Thanks to Maureen Adams, Kim Wimpsett, Jeff Kellum, and the many editors and staff at Wiley for guiding us through our first book. Thanks for your understanding when I was up against the deadlines.

Finally, the book wouldn't be complete without thanking you, our reader. We sincerely hope this book helps you to not just pass the exam, but also to be a better tech.

—Michael Aldridge

This book is the result of the hard work and support of many people. Each of the following people had a hand in making this book possible.

First, thanks to my wife, Tiffany, for her support and encouragement while I was writing this book. Thanks for putting up with the long nights and weekends.

Thanks to my mother and father for inspiring me and teaching me that I could accomplish anything I put my mind to. Thanks to Tara and Ashlee for your constant support.

Thanks to my co-author, Michael Aldridge, for his unending passion for teaching and certification, and for convincing me to follow my dream.

Thanks to James Chellis for giving us the opportunity to work on this book, and thanks to Tanner Clayton for recommending us for this book.

Thanks to Jeff Kellum, Maureen Adams, and Kim Wimpsett for guiding us through this process. Also, thanks to the many editors and staff at Wiley who helped make this book better. I feel fortunate to have been able to work with you.

Finally, thanks to you, our reader. We sincerely hope that our book helps you pass your exam and further your career.

—Josh Evitt

About the Authors

Michael Aldridge

Michael, an MCSE+I, MCSE:Security, MCDST, MCDBA, MCTS, OCP, CCNP, CCDP, CNE, SCSA, Security+, Linux+, Server+, Network+, and A+, is co-founder and President of BrainBeacon, LLC, a Nashville-based IT certification practice test provider. Michael's professional experience includes 15 years in IT in various roles, including operations analyst, technical writer, and senior network administrator. He also served in the United States Army as a 98C Intelligence Analyst.

When he can tear himself away from his children, Michael enjoys computer gaming, scuba diving, and taking in the occasional Titans or Predators game. Michael is very active in his church, singing in the choir and teaching Sunday School.

You can reach Michael at `michael@brainbeacon.com`. You can also find him as BrainBeacon Michael or TMichael on several certification forums, as he is a regular contributor to `MCSEWorld.com`, `CertCities.com`, `Tech-Unity.com`, and `CertForums.co.uk`.

Josh Evitt

Josh, an MCSE, MCSD.NET, MCAD, MCTS, MCP+I, CCDA, SCJP, CNA, and i-Net+, is co-founder and CEO of BrainBeacon, LLC, a Nashville-based IT certification practice test provider. Josh's professional experience includes over 8 years of experience in IT in various roles, including network administrator, programmer, and technical writer. When not trying to learn new technologies, Josh enjoys playing guitar and spending time with his wife Tiffany and dog Bobo.

You can reach Josh at `josh@brainbeacon.com`.

James Chellis

James Chellis, MCSE, has co-authored more than 30 IT certification titles in print. He is currently CEO of Comcourse, Inc., an online education provider.

Contents at a Glance

Contents

Introduction

Microsoft has recently changed its certification program to contain three primary series: Technology, Professional, and Architect. The Technology Series of certifications is intended to allow candidates to target specific technologies and is the basis for obtaining the Professional Series and Architect Series of certifications. The certifications contained within the Technology Series consist of one to three exams, focus on a specific technology, and do not include job-role skills. By contrast, the Professional Series of certifications focuses on a job role and is not necessarily focused on a single technology, but rather a comprehensive set of skills for performing the job role being tested. The Architect Series of certifications offered by Microsoft are premier certifications that consist of passing a review board consisting of previously certified architects. To apply for the Architect Series of certifications, you must have a minimum of 10 years of industry experience.

When obtaining a Technology Series certification, you are recognized as a Microsoft Certified Technology Specialist (MCTS) on the specific technology or technologies that you have been tested on. The Professional Series certifications include Microsoft Certified IT Professional (MCITP) and Microsoft Certified Professional Developer (MCPD). Passing the review board for an Architect Series certification will allow you to become a Microsoft Certified Architect (MCA).

This book has been developed to give you the critical skills and knowledge you need to prepare for the exam requirement for obtaining the MCTS: Windows Vista, Configuration certification: *Microsoft Windows Vista, Configuring* (Exam 70-620).

The Microsoft Certified Professional Program

Since the inception of its certification program, Microsoft has certified more than 2 million people. As the computer network industry continues to increase in both size and complexity, this number is sure to grow—and the need for *proven* ability will also increase. Certifications can help companies verify the skills of prospective employees and contractors.

Microsoft has developed its Microsoft Certified Professional (MCP) program to give you credentials that verify your ability to work with Microsoft products effectively and professionally. Several levels of certification are available based on specific suites of exams. Microsoft has recently created a new generation of certification programs:

Microsoft Certified Technology Specialist (MCTS) The MCTS can be considered the entry-level certification for the new generation of Microsoft certifications. The MCTS certification program targets specific technologies instead of specific job roles. You must take and pass one to three exams.

Microsoft Certified IT Professional (MCITP) The MCITP certification is a Professional Series certification that tests network and systems administrators on job roles, rather than only on a specific technology. The MCITP generally consists of one to three exams, in addition to obtaining an MCTS-level certification.

Microsoft Certified Professional Developer (MCPD) The MCPD certification is a Professional Series certification for application developers. Similar to the MCITP, the MCPD is focused on a job role rather than on a single technology. The MCPD generally consists of one to three exams, in addition to obtaining an MCTS-level certification.

Microsoft Certified Architect (MCA) The MCA is Microsoft's premier certification series. Obtaining the MCA requires a minimum of 10 years of experience and requires the candidate to pass a review board consisting of peer architects.

How Do You Become Certified on Windows Vista?

Attaining a Microsoft certification has always been a challenge. In the past, students have been able to acquire detailed exam information—even most of the exam questions—from online "brain dumps" and third-party "cram" books or software products. For the new generation of exams, this is simply not the case.

Microsoft has taken strong steps to protect the security and integrity of its new certification tracks. Now prospective candidates must complete a course of study that develops detailed knowledge about a wide range of topics. It supplies them with the true skills needed, derived from working with the technology being tested.

The new generations of Microsoft certification programs are heavily weighted toward hands-on skills and experience. It is recommended that candidates have troubleshooting skills acquired through hands-on experience and working knowledge.

Fortunately, if you are willing to dedicate the time and effort to learn Windows Vista, you can prepare yourself well for the exam by using the proper tools. By working through this book, you can successfully meet the exam requirements to pass the Windows Vista Configuration exam.

This book is part of a complete series of Microsoft certification Study Guides, published by Sybex Inc., that together cover the new MCTS, MCITP, MCPD exams, as well as the core MCSA and MCSE operating system requirements. Please visit the Sybex website at `www.sybex.com` for complete program and product details.

MCTS Exam Requirements

Candidates for MCTS certification on Windows Vista must pass at least one Windows Vista exam. Other MCTS certifications may require up to three exams. For a more detailed description of the Microsoft certification programs, including a list of all the exams, visit the Microsoft Learning website at `www.microsoft.com/learning/mcp`.

The *Microsoft Windows Vista Client Configuration* Exam

The Windows Vista Client Configuration exam covers concepts and skills related to installing, configuring, and managing Windows Vista computers. It emphasizes the following elements of Vista support and administration:

- Installing Vista
- Implementing and administering resources

- Implementing, managing, and troubleshooting hardware devices and drivers
- Monitoring and optimizing system performance and reliability
- Configuring and troubleshooting the Desktop environment
- Installing, configuring, and managing applications
- Implementing, managing, and troubleshooting network protocols and services
- Implementing, monitoring, and troubleshooting security

This exam is quite specific regarding Windows Vista requirements and operational settings, and it can be particular about how administrative tasks are performed within the operating system. It also focuses on fundamental concepts of Vista's operation.

In addition to being a core requirement for achieving the MCTS: Windows Vista, Configuration certification, the 70-620 exam can be used as an elective towards the MCSE or MCSE certifications on Windows 2000 or Windows Server 2003. Careful study of this book, along with hands-on experience, will help you prepare for this exam.

Microsoft provides exam objectives to give you a general overview of possible areas of coverage on the Microsoft exams. Keep in mind, however, that exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning website (`www.microsoft.com/learning/mcp`) for the most current listing of exam objectives.

Types of Exam Questions

In an effort to both refine the testing process and protect the quality of its certifications, Microsoft has focused its newer certification exams on real experience and hands-on proficiency. There is a greater emphasis on your past working environments and responsibilities and less emphasis on how well you can memorize. In fact, Microsoft says that certification candidates should have hands-on experience before attempting to pass any certification exams.

Microsoft will accomplish its goal of protecting the exams' integrity by regularly adding and removing exam questions, limiting the number of questions that any individual sees in a beta exam, limiting the number of questions delivered to an individual by using adaptive testing, and adding new exam elements.

Exam questions may be in a variety of formats: Depending on which exam you take, you'll see multiple-choice questions, as well as select-and-place and prioritize-a-list questions. Simulations and case study–based formats are included as well. You may also find yourself taking what's called an *adaptive format exam*. Let's take a look at the types of exam questions and examine the adaptive testing technique, so you'll be prepared for all of the possibilities.

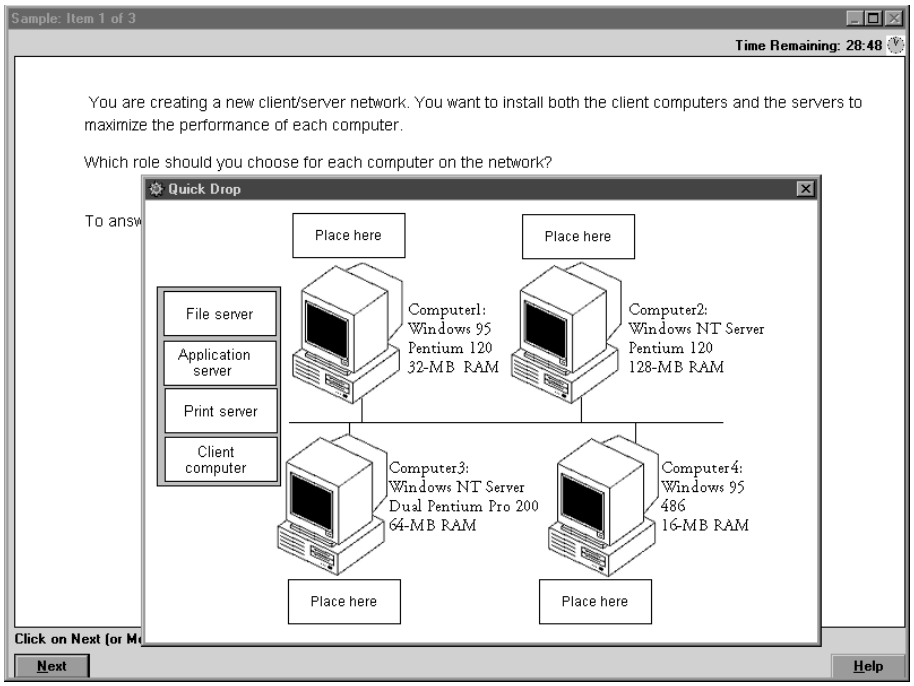
With the release of Windows 2000, Microsoft stopped providing a detailed score breakdown. This is mostly because of the various and complex question formats. Previously, each question focused on one objective. Recent exams, such as the Windows Vista Client Configuration exam, however, contain questions that may be tied to one or more objectives from one or more objective sets. Therefore, grading by objective is almost impossible. Also, Microsoft no longer offers a score. Now you will only be told if you pass or fail.

Multiple-Choice Questions

Multiple-choice questions come in two main forms. One is a straightforward question followed by several possible answers, of which one or more is correct. The other type of multiple-choice question is more complex and based on a specific scenario. The scenario may focus on several areas or objectives.

Select-and-Place Questions

Select-and-place exam questions involve graphical elements that you must manipulate to successfully answer the question. For example, you might see a diagram of a computer network, as shown in the following graphic taken from the select-and-place demo downloaded from Microsoft's website.



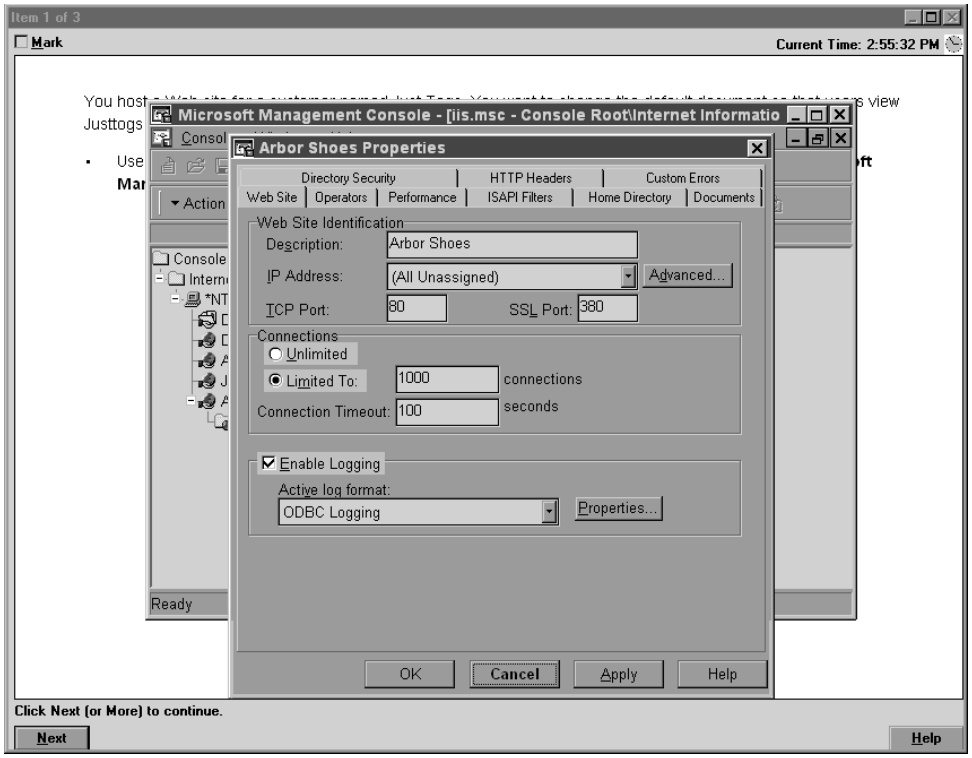
A typical diagram will show computers and other components next to boxes that contain the text "Place here." The labels for the boxes represent various computer roles on a network, such as a print server and a file server. Based on information given for each computer, you are asked to select each label and place it in the correct box. You need to place *all* of the labels correctly. No credit is given for the question if you correctly label only some of the boxes.

In another select-and-place problem you might be asked to put a series of steps in order, by dragging items from boxes on the left to boxes on the right, and placing them in the correct order. One other type requires that you drag an item from the left and place it under an item in a column on the right.

For more information on the various exam question types, go to www.microsoft.com/learning/mcpexams/policies/innovations.asp.

Simulations

Simulations are the kinds of questions that most closely represent actual situations and test the skills you use while working with Microsoft software interfaces. These exam questions include a mock interface on which you are asked to perform certain actions according to a given scenario. The simulated interfaces look nearly identical to what you see in the actual product, as shown in this example:



Because of the number of possible errors that can be made on simulations, be sure to consider the following recommendations from Microsoft:

- Do not change any simulation settings that don't pertain to the solution directly.
- When related information has not been provided, assume that the default settings are used.
- Make sure that your entries are spelled correctly.
- Close all the simulation application windows after completing the set of tasks in the simulation.

The best way to prepare for simulation questions is to spend time working with the graphical interface of the product on which you will be tested.

We recommend that you study with the WinSim Vista product, which is included on the CD that accompanies this Study Guide. By completing the exercises in this Study Guide and working with the WinSim Vista software, you will greatly improve your level of preparation for simulation questions.

Case Study–Based Questions

Case study–based questions first appeared in the MCSD program. These questions present a scenario with a range of requirements. Based on the information provided, you answer a series of multiple-choice and select-and-place questions. The interface for case study–based questions has a number of tabs, each of which contains information about the scenario. At present, this type of question appears only in most of the Design exams.

Microsoft will regularly add and remove questions from the exams. This is called *item seeding*. It is part of the effort to make it more difficult for individuals to merely memorize exam questions that were passed along by previous test-takers.

Tips for Taking the Windows Vista Client Configuration Exam

Here are some general tips for achieving success on your certification exam:

- Arrive early at the exam center so that you can relax and review your study materials. During this final review, you can look over tables and lists of exam-related information.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know *exactly* what the question is asking.
- Answer all questions. If you are unsure about a question, then mark the question for review and come back to the question at a later time.

- On simulations, do not change settings that are not directly related to the question. Also, assume default settings if the question does not specify or imply which settings are used.
- For questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. This improves your odds of selecting the correct answer when you need to make an educated guess.

Exam Registration

You may take the Microsoft exams at any of more than 1,000 Authorized Prometric Testing Centers (APTCs) and VUE Testing Centers around the world. For the location of a testing center near you, call Prometric at 800-755-EXAM (755-3926), or call VUE at 888-837-8616. Outside the United States and Canada, contact your local Prometric or VUE registration center.

Find out the number of the exam you want to take, and then register with the Prometric or VUE registration center nearest to you. At this point, you will be asked for advance payment for the exam. The exams are $125 each and you must take them within one year of payment. You can schedule exams up to six weeks in advance or as late as one working day prior to the date of the exam. You can cancel or reschedule your exam if you contact the center at least two working days prior to the exam. Same-day registration is available in some locations, subject to space availability. Where same-day registration is available, you must register a minimum of two hours before test time.

You may also register for your exams online at `www.prometric.com` or `www.vue.com`.

When you schedule the exam, you will be provided with instructions regarding appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you will receive a registration and payment confirmation letter from Prometric or VUE.

Microsoft requires certification candidates to accept the terms of a Non-Disclosure Agreement before taking certification exams.

Is This Book for You?

If you want to acquire a solid foundation in Windows Vista, and your goal is to prepare for the exam by learning how to use and manage the new operating system, this book is for you. You'll find clear explanations of the fundamental concepts you need to grasp and plenty of help to achieve the high level of professional competency you need to succeed in your chosen field.

If you want to become certified as an MCTS, this book is definitely for you. However, if you just want to attempt to pass the exam without really understanding Windows Vista, this Study Guide is *not* for you. It is written for people who want to acquire hands-on skills and in-depth knowledge of Windows Vista.

What's in the Book?

What makes a Sybex Study Guide the book of choice for hundreds of thousands of MCPs? We took into account not only what you need to know to pass the exam, but what you need to know to take what you've learned and apply it in the real world. Each book contains the following:

Objective-by-objective coverage of the topics you need to know Each chapter lists the objectives covered in that chapter.

The topics covered in this Study Guide map directly to Microsoft's official exam objectives. Each exam objective is covered completely.

Assessment Test Directly following this introduction is an Assessment Test that you should take. It is designed to help you determine how much you already know about Windows Vista. Each question is tied to a topic discussed in the book. Using the results of the Assessment Test, you can figure out the areas where you need to focus your study. Of course, we do recommend you read the entire book.

Exam Essentials To highlight what you learn, you'll find a list of Exam Essentials at the end of each chapter. The Exam Essentials section briefly highlights the topics that need your particular attention as you prepare for the exam.

Glossary Throughout each chapter, you will be introduced to important terms and concepts that you will need to know for the exam. These terms appear in italic within the chapters, and at the end of the book, a detailed Glossary gives definitions for these terms, as well as other general terms you should know.

Review questions, complete with detailed explanations Each chapter is followed by a set of Review Questions that test what you learned in the chapter. The questions are written with the exam in mind, meaning that they are designed to have the same look and feel as what you'll see on the exam. Question types are just like the exam, including multiple choice, exhibits, and select-and-place.

Hands-on exercises In each chapter, you'll find exercises designed to give you the important hands-on experience that is critical for your exam preparation. The exercises support the topics of the chapter, and they walk you through the steps necessary to perform a particular function.

Real World Scenarios Because reading a book isn't enough for you to learn how to apply these topics in your everyday duties, we have provided Real World Scenarios in special sidebars. These explain when and why a particular solution would make sense, in a working environment you'd actually encounter.

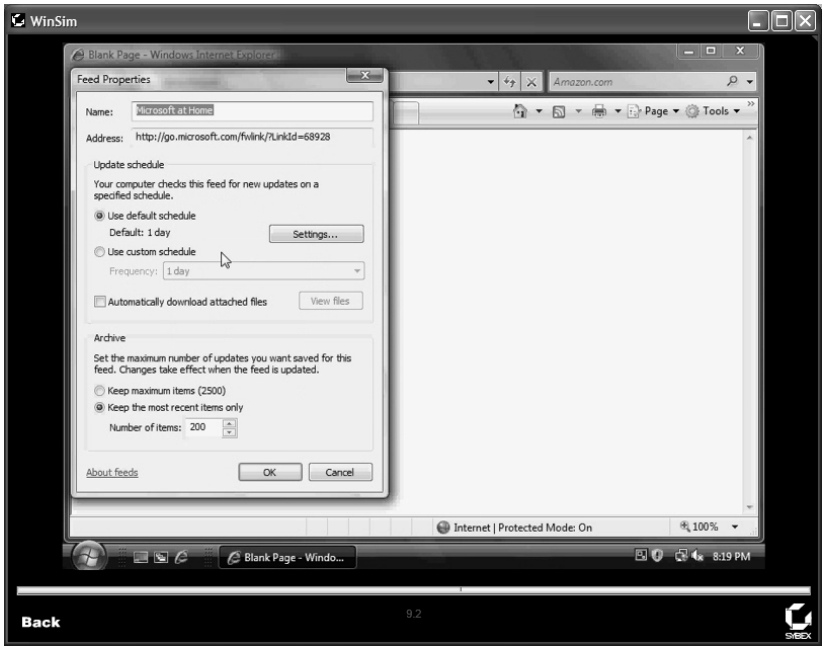
Interactive CD Every Sybex Study Guide comes with a CD complete with additional questions, flashcards for use with an interactive device, a Windows simulation program, and the book in electronic format. Details are in the following section.

What's on the CD?

With this new member of our best-selling Study Guide series, we are including quite an array of training resources. The CD offers numerous simulations, bonus exams, and flashcards to help you study for the exam. We have also included the complete contents of the Study Guide in electronic form. The CD's resources are described here:

The Sybex E-book for Windows Vista Many people like the convenience of being able to carry their whole Study Guide on a CD. They also like being able to search the text via computer to find specific information quickly and easily. For these reasons, the entire contents of this Study Guide are supplied on the CD, in PDF. We've also included Adobe Acrobat Reader, which provides the interface for the PDF contents as well as the search capabilities.

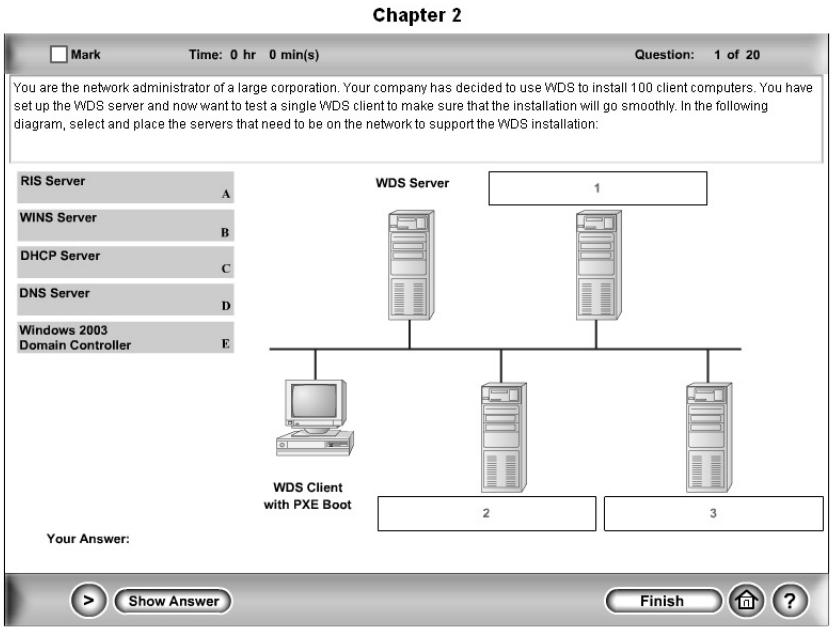
WinSim Vista We developed the WinSim Vista product to allow you to experience the multimedia and interactive operation of working with Windows Vista. WinSim Vista provides both audio/video files and hands-on experience with key features of Windows Vista. Built around the Study Guide's exercises, WinSim Vista will help you attain the knowledge and hands-on skills you must have in order to understand Windows Vista (and pass the exam). Here is a sample screen from WinSim Vista:



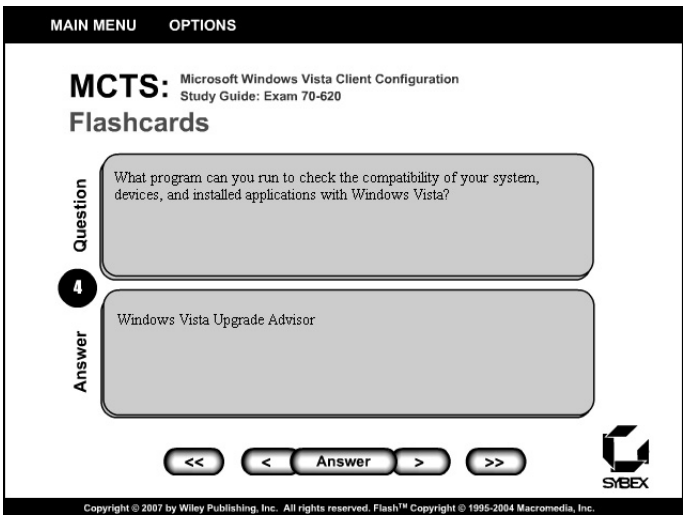
The Sybex Test Engine This is a collection of multiple-choice questions that will help you prepare for your exam. There are four sets of questions:

- Two bonus exams designed to simulate the actual live exam.
- All the questions from the Study Guide, presented in a test engine for your review. You can review questions by chapter or by objective, or you can take a random test.
- The Assessment Test.

Here is a sample screen from the Sybex Test Engine:



Sybex Flashcards for PCs and Handheld Devices The "flashcard" style of question offers an effective way to quickly and efficiently test your understanding of the fundamental concepts covered in the exam. The Sybex Flashcards set consists of 150 questions presented in a special engine developed specifically for this Study Guide series. Here's what the Sybex Flashcards interface looks like:



Because of the high demand for a product that will run on handheld devices, we have also developed, in conjunction with Land-J Technologies, a version of the flashcard questions that you can take with you on your Palm OS PDA (including the PalmPilot and Handspring's Visor).

Hardware and Software Requirements

You should verify that your computer meets the minimum requirements for installing Windows Vista as listed in Table 1.1 in Chapter 1. We suggest that your computer meets or exceeds the recommended requirements for a more enjoyable experience.

The exercises in this book assume that your computer is configured in a specific manner. Your computer should have at least a 20GB drive that is configured with the minimum space requirements and partitions. Other exercises in this book assume that your computer is configured as follows:

- 20GB C: partition with the NTFS file system
- Optional D: partition with the FAT32 file system
- 15GB or more of free space

Of course, you can allocate more space to your partitions if it is available.

The first exercise in the book assumes that you are performing a clean installation and not an upgrade. Your partitions should be created and formatted as previously specified.

Contacts and Resources

To find out more about Microsoft Education and Certification materials and programs, to register with Prometric or VUE, or to obtain other useful certification information and additional study resources, check the following resources:

Microsoft Learning Home Page

www.microsoft.com/learning

This website provides information about the MCP program and exams. You can also order the latest Microsoft Roadmap to Education and Certification.

Microsoft TechNet Technical Information Network

www.microsoft.com/technet

800-344-2121

Use this website or phone number to contact support professionals and system administrators. Outside the United States and Canada, contact your local Microsoft subsidiary for information.

PalmPilot Training Product Development: Land-J

www.land-j.com

407-359-2217

Land-J Technologies is a consulting and programming business currently specializing in application development for the 3Com PalmPilot Personal Digital Assistant. Land-J developed the Palm version of the EdgeTests, which is included on the CD that accompanies this Study Guide.

Prometric

www.prometric.com

800-755-3936

Contact Prometric to register to take an MCP exam at any of more than 800 Prometric Testing Centers around the world.

Virtual University Enterprises (VUE)

www.vue.com

888-837-8616

Contact the VUE registration center to register to take an MCP exam at one of the VUE Testing Centers.

MCP Magazine Online

www.mcpmag.com

Microsoft Certified Professional Magazine is a well-respected publication that focuses on Windows certification. This site hosts chats and discussion forums and tracks news related to the MCSE program. Some of the services cost a fee, but they are well worth it.

Windows & .NET Magazine

www.windows2000mag.com

You can subscribe to this magazine or read free articles at the website. The study resource provides general information on Windows 2000, XP, and .NET Server.

BrainBeacon Practice Exams

www.brainbeacon.com

BrainBeacon offers IT certification exam preparation materials for Microsoft exams.

Assessment Test

1. What extension is applied by default to custom consoles that are created for the MMC?
   - **A.** `.mmc`
   - **B.** `.msc`
   - **C.** `.con`
   - **D.** `.mcn`

2. You want to create roaming profiles for users in the sales department. They frequently log on at computers in a central area. The profiles should be configured as mandatory and roaming profiles. Which users are able to manage mandatory profiles on Windows Vista computers?
   - **A.** The user who uses the profile
   - **B.** Server operators
   - **C.** Power users
   - **D.** Administrators

3. You want to monitor the CPU, memory, and disk usage on your computer to ensure that there are no bottlenecks. Which MMC snap-in would you load to access System Monitor?
   - **A.** System Monitor
   - **B.** Reliability Monitor
   - **C.** ActiveX Control
   - **D.** Performance Logs and Alerts

4. If you wanted to require that a user enter an Administrator password in order to perform administrative tasks, then what type of user account should you create for the user?
   - **A.** Administrator User account
   - **B.** Standard User account
   - **C.** Power User account
   - **D.** Authenticated User account

5. You have installed a clean installation of Windows Vista on your computer. You want to create an image of the new installation to use as a basis for remote installs. What Windows Vista utility should you use to accomplish this?
   - **A.** WDS
   - **B.** Windows SIM
   - **C.** ImageX
   - **D.** Sysprep

6. Which of the following statements is true regarding the built-in Administrator account in Windows Vista? (Choose all that apply.)
   - **A.** The built-in Administrator account does not exist in Windows Vista.
   - **B.** The built-in Administrator account is disabled by default in Windows Vista.
   - **C.** The built-in Administrator account has no permissions in Windows Vista.
   - **D.** The built-in Administrator account not a member of the Administrators group in Windows Vista.

7. You have a user with limited vision. Which accessibility utility is used to read aloud screen text, such as the text in dialog boxes, menus, and buttons?
   - **A.** Read-Aloud
   - **B.** Orator
   - **C.** Dialog Manager
   - **D.** Narrator

8. You have just purchased a new computer that has Windows Vista preinstalled. You want to migrate existing users from your previous computer that was running Windows XP Professional. Which two files would you use to manage this process through the User State Migration Tool?
   - **A.** `usmt.exe`
   - **B.** `ScanState.exe`
   - **C.** `LoadState.exe`
   - **D.** `vistaMigrate.exe`

9. You have scheduled a specific program that is required by the accounting department to run as a scheduled task every day. When you log on as an administrator, you can run the task, but when the scheduled task is supposed to run, it does not run properly. You have already verified that the Task Scheduler task is running. What else should you check?
   - **A.** Verify that the task has been configured to run in unattended mode.
   - **B.** Make sure the user who is scheduled to run the task has the appropriate permissions.
   - **C.** Make sure that the time is properly synchronized on the computer.
   - **D.** Verify that the Process Manager task is running.

10. You are the network administrator for your company. Recently, one of your users in the Accounting department has reported that they were unsure whether a banking website was legitimate or not. You want to configure a utility that will verify whether a website is known to be fraudulent. Which utility should you configure?
    - **A.** Pop-up Blocker
    - **B.** RSS Reader
    - **C.** Phishing Filter
    - **D.** Add-on Manager

11. You have a user, Jan, who suspects that her Windows Vista computer has been infected with spyware. You remove the spyware from her computer, and you want to prevent spyware from infecting the computer in the future. Which of the following Vista utilities should you configure?

A. Windows Defender

B. Phishing Filter

C. Pop-up Blocker

D. Windows OneCare

12. You are configuring power settings on your laptop. You configure the laptop to enter sleep mode after a specified period of inactivity. Which of the following will occur when the computer enters sleep mode?

A. The computer will be shut down gracefully.

B. Data will be saved to the hard disk.

C. The monitor and hard disk will be turned off, but the computer will remain in a fully active state.

D. The user session will not be available when you resume activity on the computer.

13. You are using Internet Explorer to access several RSS feeds that you are subscribed to. One of the feeds only stores the 10 most recent updates to the feed. You want to ensure that the last 100 updates are stored. What should you do?

A. Configure the RSS feed to automatically download attached files.

B. Modify the schedule so that the RSS feed is update more than once a day.

C. Turn on feed reading view in IE.

D. Modify the archive setting so that the last 100 items are stored.

14. You are using Windows Mail on your Windows Vista computer. You want to prevent advertisements from a company you no longer do business with from being sent to your inbox. Which of the following should you do?

A. Move all messages from the company to the Junk Mail folder.

B. Move all messages from the company to the Deleted Items folder.

C. Remove the company's domain from the Safe Senders list.

D. Add the company's domain to the Blocked Senders list.

15. You are configuring a new Windows Vista computer for a new employee. You configure the new user with a Standard User account. Which of the following functions will the new employee be allowed to perform?

A. Install a printer.

B. Install network drivers.

C. Configure WPA keys.

A. Modify the desktop settings.

16. You are the network administrator for BrainBeacon. Your network consists of 200 Windows Vista computers, and you want to assign static IP addresses rather than use a DHCP server. You want to configure the computers to reside on the 192.168.10.0 network. What subnet mask should you use with this network address?
    - **A.** 255.0.0.0
    - **B.** 255.255.0.0
    - **C.** 255.255.255.0
    - **D.** 255.255.255.255

17. You are using a laptop running Windows Vista Home Premium. You want to synchronize files between your laptop and a network folder. Which of the following actions must you perform first in order to enable synchronization to occur between your laptop and the network folder?
    - **A.** Upgrade your laptop to Windows Vista Ultimate.
    - **B.** Enable one-way synchronization between the laptop and the network folder.
    - **C.** Enable two-way synchronization between the laptop and the network folder.
    - **D.** Configure the files on your laptop as read only.

18. You have a DNS server that contains corrupt information. You fix the problem with the DNS server, but one of your users is complaining that they are still unable to access Internet resources. You verify that everything works on another computer on the same subnet. Which command can you use to fix the problem?
    - **A.** `IPCONFIG /flush`
    - **B.** `IPCONFIG /flushdns`
    - **C.** `PING /flush`
    - **D.** `GROPE /flushdns`

19. Which of the following information can be configured on a VPN client so that it can access a VPN server? (Choose two answers.)
    - **A.** IP address
    - **B.** MAC address
    - **C.** Domain name
    - **D.** Connection address

20. Which of the following statements is true regarding the creation of a group in Windows Vista?
    - **A.** Only members of the Administrators group can create users on a Windows Vista computer.
    - **B.** Group names can be up to 64 characters.
    - **C.** Group names can contain spaces.
    - **D.** Group names can be the same as usernames but not the same as other group names on the computer.

21. You need to expand the disk space on your Windows Vista computer. You are considering using spanned volumes. Which of the following statements is/are true concerning spanned volumes? (Choose all that apply.)

A. Spanned volumes can contain space from 2 to 32 physical drives.

B. Spanned volumes can contain space from 2 to 24 physical drives.

C. Spanned volumes can be formatted as FAT32 or NTFS partitions.

D. Spanned volumes can be formatted only as NTFS partitions.

22. Which of the following versions of Windows Vista support the Windows Aero interface? (Choose all that apply.)

A. Windows Vista Home Basic

B. Windows Vista Home Premium

C. Windows Vista Business

D. Windows Vista Ultimate

23. Your home computer network is protected by a firewall. You have configured your Windows Vista home computer to use Windows Mail. After you configure your e-mail accounts, you discover that you are unable to send e-mail messages from Windows Mail. Your e-mail provider uses POP3 and SMTP. What port should you open on the firewall?

A. 25

B. 110

C. 443

D. 995

24. You are configuring Windows Sidebar on your computer. You have two monitors, and you want to ensure that the sidebar is always displayed on the left side of monitor 2. Which of the following settings should you configure?

A. No configuration changes will be necessary.

B. Configure Windows Sidebar to be displayed on the left side of the screen and on monitor 2.

C. Configure Windows Sidebar to always be displayed on top of other windows.

D. Configure Windows Sidebar to be displayed on monitor 1.

25. Which of the following versions of Windows Vista can be upgraded to Windows Vista Ultimate Edition? (Choose all that apply.)

A. Windows Vista Home Starter

B. Windows Vista Home Basic

C. Windows Vista Home Premium

D. Windows Vista Business

26. You are configuring a Windows Vista computer that is going to be used by your children. You are configuring access restrictions using the Parental Controls feature of Windows Vista. Which of the following can be configured by setting Parental Controls? (Choose all that apply.)

A. When your children can access the computer

B. What websites your children can view

C. What programs your children can access

D. What other computers on your home network your children can access

27. How do you access the Advanced Boot Menu in Windows Vista during the boot process?

A. Press the spacebar.

B. Press F6.

C. Press F8.

D. Press F10.

28. You use Windows CardSpace to manage the information you provide to websites. Because security is important to you, you want to further protect your card information. Which of the following should you do to further protect your card?

A. Encrypt the card data.

B. Create a unique PIN for the card.

C. Create a managed card, and encrypt the contents of the managed card.

D. Create a managed card, and create a unique PIN for the managed card.

29. Which utility is used to upgrade a FAT32 partition to NTFS?

A. UPFS

B. UPGRADE

C. Disk Manager

D. CONVERT

30. You want to be able to track which users are accessing the `C:\PAYROLL` folder and whether the access requests are successful. Which of the following audit policy options allows you to track events related to file and print object access?

A. File and Object Access

B. Audit Object Access

C. Audit File and Print Access

D. Audit All File and Print Events

Answers to Assessment Test

1. B. When you create a custom console for the MMC, the `.msc` filename extension is automatically applied. See Chapter 3 for more information.

2. D. Only members of the Administrators group can manage mandatory profiles. See Chapter 5 for more information.

3. C. Select ActiveX Control in the Add/Remove Snap-in dialog box. Then, from the Insert ActiveX Control dialog box, select System Monitor Control to access the System Monitor utility. You can also access the System Monitor view by opening Performance Monitor. See Chapter 11 for more information.

4. B. You would create a Standard User account for the user. Standard users must provide the credentials of an Administrator account when prompted by User Account Control (UAC) in order to perform administrative tasks. See Chapter 5 for more information.

5. C. You can use the ImageX utility to create an image of a Windows Vista installation. After the image has been created, you can prepare the image with a utility such as the System Preparation Tool (Sysprep). The image can then be used for remote installations of Windows Vista. See Chapter 2 for more information.

6. B. The built-in Administrator account is disabled by default in Windows Vista. However, it can be enabled through Local Users and Groups or by modifying the Accounts: Administrator Account Status GPO setting. See Chapter 5 for more information.

7. D. The Narrator utility uses a sound output device to read on-screen text. See Chapter 4 for more information.

8. B, C. Windows Vista ships with a utility called the User State Migration Tool (USMT) that is used by administrators to migrate users from one computer to another via a command-line utility. The USMT consists of two executable files: `ScanState.exe` and `LoadState.exe`. See Chapter 1 for more information.

9. B. If you are using Task Scheduler and your jobs are not running properly, make sure that the Task Scheduler service is running and is configured to start automatically. You should also ensure that the user who configured to run the scheduled task has sufficient permissions to run the task. See Chapter 11 for more information.

10. C. Internet Explorer 7 ships with Phishing Filter, which can help verify whether a website is known to be fraudulent or not. Phishing Filter helps to prevent malicious websites from masquerading as a legitimate site in order to obtain your personal or financial information. See Chapter 9 for more information.

11. A. Windows Defender is an antispyware program included with Windows Vista. Windows Defender offers real-time protection from spyware and other unwanted software. You can also configure Windows Defender to scan for spyware on a regular basis. See Chapter 6 for more information.

12. B. Sleep mode is a combination of Standby mode and Hibernate mode. When sleep mode is configured, the user's session is quickly accessible on wakeup, but the data is saved to the hard disk. Sleep mode is the preferred power-saving mode in Windows Vista. See Chapter 3 for more information.

13. D. Internet Explorer 7 provides the ability to read and subscribe to RSS feeds. You can configure several options for RSS feeds, such as how often the feed is checked for updates, whether attachments are automatically downloaded, and how many updates are stored for the feed. See Chapter 9 for more information.

14. D. To prevent messages from a company from being delivered to your inbox, you should add the company's domain to the Blocked Senders list. By adding a domain to the Blocked Senders list, messages from that domain will be delivered to the Junk Mail folder rather than the inbox. See Chapter 10 for more information.

15. A, C, D. Standard users are allowed to perform a variety of tasks, such as install printers, configure wireless keys, and modify their desktop settings. See Chapter 6 for more information.

16. C. You should use the subnet mask 255.255.255.0 on your network in this scenario. The IP network address 192.168.10.0 is a Class C address. Class C addresses, by default, use the subnet mask 255.255.255.0. The network portion of the address is 192.168.10, and the host portion of the address can be 1-254. See Chapter 8 for more information.

17. A. In order to enable synchronization of files between your laptop and a network folder, you must first upgrade your laptop to a version of Windows Vista, such as Windows Vista Ultimate, that supports synchronization with network folders. Windows Sync Center also supports synchronization of files between computers and mobile devices. See Chapter 10 for more information.

18. B. The `IPCONFIG /flushdns` command is used to purge the DNS Resolver cache. The `IPCONFIG` command displays a computer's IP configuration. See Chapter 8 for more information.

19. A, C. When you configure a VPN connection, you must specify the IP address or host domain name of the computer to which you'll connect. See Chapter 8 for more information.

20. A, C. Only Administrators can create new groups on a Windows Vista computer. Group names can contain up to 256 characters and can contain spaces. Group names must be unique to the computer, different from all the other usernames and group names that have been specified on that computer. See Chapter 5 for more information.

21. A, C. You can create a spanned volume from free space that exists on a minimum of 2 to a maximum of 32 physical drives. When the spanned volume is initially created in Windows Vista, it can be formatted with FAT32 or NTFS. If you extend a volume that already contains data, however, the partition must be NTFS. See Chapter 7 for more information.

22. B, C, D. The new Windows Aero interface is not available on Windows Vista Home Basic. It is available on Windows Vista Home Premium, Windows Vista Business, and Windows Vista Ultimate. See Chapter 1 for more information.

23. A. Port 25 should be opened on the firewall. SMTP is used for outbound mail and uses port 25. POP3, which is used for receiving inbound mail, uses port 110. See Chapter 10 for more information.

24. B. You should configure Windows Sidebar to be displayed on the left side of the screen, and on monitor 2. You can configure several options for Windows Sidebar, such as which monitor Sidebar is displayed on, which side of the monitor Sidebar is displayed on, whether Sidebar should appear on top of other windows, and whether Sidebar should start when Windows starts. See Chapter 4 for more information.

25. B, C, D. You can upgrade Windows Vista Home Basic, Windows Vista Home Premium, and Windows Vista Business to Windows Vista Ultimate Edition. See Chapter 1 for more information.

26. A, B, C. Using Parental Controls, you can configure what websites your children can access, when they can use the computer, what games they can play, what programs they can run, and you can view reports regarding their activity. See Chapter 9 for more information.

27. C. During the boot process, you are prompted to press F8 to access the Advanced Boot Menu. See Chapter 11 for more information.

28. B. You should create a unique PIN for the card. By default, cards are encrypted on your computer, but you can further secure them by creating a unique PIN. PINs must be at least four characters long and can consist of uppercase and lowercase letters, numbers, symbols, and spaces. You cannot create a managed card. See Chapter 10 for more information.

29. D. The CONVERT utility is used to convert a FAT32 partition to NTFS. See Chapter 7 for more information.

30. B. Though all four options seem plausible, only the Audit Object Access option actually exists. Audit Object Access is used to enable auditing of access to files, folders, and printers. Once you enable auditing of object access, you must enable file auditing through NTFS security, or enable print auditing through printer security. See Chapter 6 for more information.

Chapter 1

Getting Started with Windows Vista

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Installing and Upgrading Windows Vista**
  - Identify hardware requirements
  - Perform a clean installation
  - Upgrade to Windows Vista from previous versions of Windows
  - Upgrade from one edition of Windows Vista to another edition
  - Troubleshoot Windows Vista installation issues
  - Install and configure Windows Vista drivers
- ✓ **Maintaining and Optimizing Systems that Run Windows Vista**
  - Configure Windows Update

Preparing for an installation involves making sure that your hardware meets the minimum requirements and that your hardware is supported by Windows Vista. When you install Windows Vista, you should also decide whether you are upgrading or installing a clean copy on your computer. An upgrade attempts to preserve existing settings; a clean install puts a fresh copy of the operating system on your computer. Installation preparation also involves making choices about your system's configuration, such as selecting a disk-partitioning scheme.

Once you've completed all the planning, you are ready to install Vista. This is a straightforward process that is highly automated and user friendly.

To complete the Windows Vista installation, you will need to activate the product through Windows Activation. This process is used to reduce software piracy. After Windows Vista is installed, you can keep the operating system up-to-date with post-installation updates.

When you install Windows Vista, you should also consider whether the computer will be used for dual-boot or multi-boot purposes. Dual-booting or multi-booting allows you to have your computer boot with operating systems other than Windows Vista.

Preparing to Install Windows Vista

Windows Vista is easy to install. But this doesn't mean you don't need to prepare for the installation process. Before you begin, you should know what is required for a successful installation and have all the pieces of information you'll need to supply during the installation process. In preparing for the installation, you should make sure that you do the following:

- Understand the differences between Windows Vista editions.
- Know the hardware requirements for Windows Vista.
- Know how to use the Windows Vista Upgrade Advisor and the Hardware Compatibility List (HCL) to determine whether your hardware is supported by Windows Vista.
- Have verification that your computer's BIOS is compatible with Windows Vista.
- Know whether the devices in your computer have Windows Vista drivers.
- Understand the difference between a clean install and an upgrade.
- Decide whether you want to migrate user data.
- Know the installation options suitable for your system, including which disk-partitioning scheme you should select for Windows Vista to use.

The following sections describe the preparation that is required prior to installing Windows Vista.

Windows Vista Editions

Windows Vista is available in six editions:

- Windows Vista Starter
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate

Multiple editions will be contained on the Windows Vista media, and you can unlock which one you want based on the product key.

All editions of Windows Vista are available for the Intel *x*86-based 32-bit processor architecture. All editions of Vista except Vista Starter are available for the 64-bit *x*64-based processor architecture; Vista Starter is available only for 32-bit architectures.

Windows Vista supports computers with one or two physical processors. Windows Vista Starter, Windows Vista Home Basic, and Windows Vista Home Premium will support one physical processor. Windows Vista Business, Windows Vista Enterprise, and Windows Vista Ultimate will support two physical processors. There is no limit to the number of processor cores these editions will support, so you will be able to use quad-core processor architectures with Windows Vista.

Windows Vista Starter will be available only to emerging markets, where software piracy typically runs rampant; Windows Vista Starter will not be available in the United States or Europe. It has the following limitations:

- Only three applications can be launched simultaneously.
- Incoming network connections are blocked.
- Memory is limited to 2GB.
- Only 32-bit processor architectures are available.
- Only a single Celeron, Pentium III, or equivalent processor is supported.

Windows Vista Home Basic is recommended for basic computer needs, such as accessing the Internet, checking e-mail, and basic document creation. Home Basic has the following features and limitations:

- Windows Aero (the new user interface) is not available.
- Only a single physical processor can be installed.
- Memory is limited to 8GB.

Windows Vista Home Premium includes digital entertainment features. Home Premium has the following features and limitations:

- All of the features found in Windows Vista Home Basic
- Windows Aero
- Integrated operating system search functionality
- Windows Media Center capabilities, which can be used to record and watch TV and HDTV, and to connect the PC with an Xbox 360
- Windows Tablet PC capabilities, which can be used to enable digital pen and touchscreen interfaces
- Integrated DVD authoring
- Extra games
- File system encryption
- Photo management application
- Limited to a single physical processor
- Memory limited to 16GB

Windows Vista Business is similar in functionality to Windows XP Professional. It contains the following features and limitations:

- Does not include Media Center capabilities
- Windows Aero
- Integrated operating system search functionality
- Windows Tablet PC capabilities, which can be used to enable digital pen and touchscreen interfaces
- IIS web server
- Offline file support
- Fax support
- Remote Desktop support
- Previous versions support
- Dual physical processor support
- Memory limited to 128GB

Windows Vista Enterprise includes the following features and limitations:

- All of the features found in Windows Vista Business
- Virtual PC Express
- BitLocker Drive Encryption
- Subsystem for Unix-based applications

- Inclusion of all user-interface languages available to Windows
- Only available via Microsoft Software Assurance or a Microsoft Enterprise Agreement

Windows Vista Ultimate has everything that Windows Vista has to offer, including the following:

- All of the features found in Windows Vista Home Premium
- All of the features found in Windows Vista Enterprise
- DVD ripping support
- Podcast creation support
- WinSAT, which is used to improve gaming performance

Two more editions, Windows Vista Home Basic N and Windows Vista Business N, will be available only in the European Union. These editions will ship without Windows Media Player.

You can use a Control Panel tool named Windows Anytime Upgrade to purchase a one-time upgrade license to a more advanced edition of Windows Vista. You can upgrade Home Basic to Home Premium or Ultimate, you can upgrade Home Premium to Ultimate, and you can upgrade Business to Ultimate. We will discuss Windows Anytime Upgrade in detail later in the chapter.

For the exercises and screen captures throughout this book, we will be using Windows Vista Ultimate.

Hardware Requirements

To install Windows Vista successfully, your system must meet certain hardware requirements. Table 1.1 lists the requirements for a Windows Vista Capable PC as well as the requirements for a Windows Vista Premium Ready PC.

TABLE 1.1 Hardware Requirements (Non-network Installation)

Component	Windows Vista Capable PC	Windows Vista Premium Ready PC
Processor	800MHz 32-bit (*x*86) or 64-bit (*x*64) processor; Intel Core/Pentium/ Celeron, AMD, Via, or compatible	1GHz 32-bit (x86) or 64-bit (x64) processor; Intel Core/Pentium/Celeron, AMD, Via, or compatible
Memory	512MB	1GB

TABLE 1.1 Hardware Requirements (Non-network Installation) *(continued)*

Component	Windows Vista Capable PC	Windows Vista Premium Ready PC
Disk space	20GB hard drive with 15GB of free disk space	40GB hard drive with 15GB free disk space
Graphics	DirectX 9 video card capable of SVGA at 800×600 resolution (WDDM Driver Support recommended)	DirectX 9 video card that supports a WDDM driver, Pixel Shader 2.0 in hardware, and 32 bits per pixel; graphics card memory dependent on desired resolution
Optical drive	Internal or external CD or DVD drive	Internal or external DVD drive

A Windows Vista Capable PC meets or exceeds the basic requirements to deliver the core functionality of Windows Vista. These requirements assume that you are installing only the operating system without any premium functionality. For example, you may be able to get by with the minimum requirements if you are installing the operating system just to learn the basics of the software.

A Windows Vista Premium Ready PC is able to use premium Windows Vista features, such as Windows Aero. The requirements for the graphic card depend on the resolution at which you want to run. The required amount of memory is as follows:

- 64MB is required for a single monitor at a resolution of 1,310,720 pixels or less, which is equivalent to a 1280×1024 resolution.
- 128MB is required for a single monitor at a resolution of 2,304,000 pixels or less, which is equivalent to a 1920×1200 resolution.
- 256MB is required for a single monitor at a resolution larger than 2,304,000 pixels.

In addition, the graphics memory bandwidth must be at least 1,600MB per second, as assessed by the Windows Vista Upgrade Advisor.

If you choose to install Windows Vista from the network, you will also need a network connection and a server with the distribution files.

Since computer technology and the standard for acceptable performance are constantly changing, the recommendations are somewhat subjective. However, the recommended hardware requirements are based on the standards at the time that Windows Vista was released.

The hardware requirements listed in Table 1.1 were those specified at the time this book was published. Check Microsoft's website at `www.microsoft.com/technet/windowsvista/evaluate/hardware/vistarpc.mspx` for the most current information.

Real World Scenario

Deciding on Minimum Hardware Requirements

The company you work for has decided that everyone will have their own laptop running Windows Vista. You need to decide on the new computers' specifications for processor, memory, and disk space.

The first step is to determine which applications will be used. Typically, most users will work with an e-mail program, a word processor, a spreadsheet, presentation software, and maybe a drawing or graphics program. Additionally, an antivirus application will probably be used. Under these demands, an 800MHz Celeron processor and 512MB of RAM will make for a very slow-running machine. So for this usage, you can assume that the minimum baseline configuration would be a Pentium 4 processor with 1GB of RAM.

Based on your choice of baseline configuration, you should then fit a test computer with the applications that will be used on it and test the configuration in a lab environment simulating normal use. This will give you an idea whether the RAM and processor calculations you have made for your environment are going to provide suitable response.

Today's disk drives have become capable of much larger capacity while dropping drastically in price. So for disk space, the rule of thumb is to buy whatever is the current standard. At the time this book was published, 80GB drives were commonplace, which is sufficient for most users. If users plan to store substantial graphics or video files, you may need to consider buying larger-than-standard drives.

Also consider what the business requirements will be over the next 12 to 18 months. If you will be implementing applications that are memory or processor intensive, you may want to spec out the computers with hardware sufficient to support upcoming needs, to avoid costly upgrades in the near future.

Measurement Units Used in Hardware Specifications

Computer processors are typically rated by speed. The speed of the processor, or *central processing unit (CPU)*, is rated by the number of clock cycles that can be performed in one second. This measurement is typically expressed in *gigahertz (GHz)*. One GHz is one trillion cycles per second. Keep in mind that processor architecture must also be taken into account when considering processor speed. A processor with a more efficient pipeline will be faster than a processor with a less efficient pipeline at the same CPU speed.

Hard disks are commonly rated by capacity. The following measurements are used for disk space and memory capacity:

1*MB (megabyte)* = 1024KB (*kilobytes*)

1*GB (gigabyte)* = 1024MB

1*TB (terabyte)* = 1024GB

1*PB (petabyte)* = 1024TB

1*EB (exabyte)* = 1024PB

The Hardware Compatibility List (HCL)

Along with meeting the minimum requirements, your hardware should appear on the *Hardware Compatibility List (HCL)*. The HCL is an extensive list of computers and peripheral hardware that have been tested with the Windows Vista operating system.

The Windows Vista operating system requires control of the hardware for stability, efficiency, and security. The hardware and supported drivers on the HCL have been put through rigorous tests to ensure their compatibility with Windows Vista. Microsoft guarantees that the items on the list meet the requirements for Windows Vista and do not have any incompatibilities that could affect the stability of the operating system.

If you call Microsoft for support, the first thing a Microsoft support engineer will ask about is your configuration. If you have any hardware that is not on the HCL, you may not be able to get support from Microsoft.

To determine if your computer and peripherals are on the HCL, check the most up-to-date list at `https://winqual.microsoft.com/HCL/Default.aspx`.

BIOS Compatibility

Before you install Windows Vista, you should verify that your computer has the most current BIOS (Basic Input/Output System). This is especially important if your current BIOS does not include support for Advanced Configuration and Power Interface (ACPI) functionality. ACPI functionality is required for Windows Vista to function properly. Check the computer's vendor for the latest BIOS version information.

Driver Requirements

To successfully install Windows Vista, you must have the critical device drivers for your computer, such as the hard drive device driver. The Windows Vista media comes with an extensive list of drivers. If your computer's device drivers are not on the Windows Vista installation media, you should check the device manufacturer's website. If you can't find the device driver on the manufacturer's website and no other compatible driver exists, you are out of luck. Windows Vista will not recognize devices that don't have Windows Vista drivers.

Clean Install or Upgrade?

Once you've determined that your hardware meets the minimum requirements, you need to decide whether you want to do an upgrade or a *clean install*.

An *upgrade* allows you to retain your existing operating system's applications, settings, and files. If you currently have a computer with Windows 2000 Professional or Windows XP Professional, you are eligible to purchase an upgrade copy of Windows Vista. However, you must perform a clean install with Windows 2000 Professional.

You can perform an upgrade if the following conditions are true:

- You are running Windows XP.
- You want to keep your existing applications and preferences.
- You want to preserve any local users and groups you've created.

You must perform a clean install if any of the following conditions are true:

- There is no operating system currently installed.
- You have an operating system installed that does not support an in-place upgrade to Windows Vista (such as DOS, Windows 9*x*, Windows NT, Windows Me, or Windows 2000 Professional).
- You want to start from scratch, without keeping any existing preferences.
- You want to be able to dual-boot between Windows Vista and your previous operating system.

Only certain versions of Windows will allow an in-place upgrade to Windows Vista. Generally, if the Windows Vista installation would cause your existing installation to lose functionality, a clean install must occur. Table 1.2 shows the operating systems that can be upgraded to each edition of Windows Vista.

TABLE 1.2 Windows Vista Upgrade Options

	Home Basic	Home Premium	Business	Ultimate
Windows 2000 Professional	No	No	No	No
Windows XP Home	Yes	Yes	Yes	Yes
Windows XP Media Center	No	Yes	No	Yes
Windows XP Professional	No	No	Yes	Yes
Windows XP Tablet PC	No	No	Yes	Yes
Windows XP Professional *x*64	No	No	No	No

Other operating systems cannot be upgraded, but they may be able to coexist with Windows Vista in a dual-boot or multi-boot environment. These operating systems require that you purchase a full version of Windows Vista.

Dual-booting and multibooting are covered in the "Supporting Multiple-Boot Options" section later in this chapter.

If you don't have an operating system that can be upgraded, or if you want to keep your previous operating system intact, you need to perform a clean install. A clean install puts the Windows Vista operating system into a new folder and uses its default settings the first time the operating system is loaded. After a clean install, you will need to reinstall all your applications and reset your preferences.

If you are performing a clean install to the same partition as an existing version of Windows, the contents of the existing `Users` (or `Documents and Settings`), `Program Files`, and `Windows` directories will be placed in a directory named `Windows.old`, and the old operating system will no longer be available.

Upgrade Considerations

Almost all Windows 2000 Professional and Windows XP applications should run with Windows Vista. However, the following are a few exceptions to this statement:

- Applications that use file-system filters, such as antivirus software, may not be compatible.
- Custom power-management tools are not supported.
- Custom Plug and Play solutions are not supported.
- Before upgrading to Windows Vista, you should remove any virus scanners, network services, or other client software.

Hardware Compatibility Issues

You need to ensure that you have Windows Vista device drivers for your hardware. If you have a video driver without a Windows Vista–compatible driver, the Windows Vista upgrade will install the Standard VGA driver, which will display the video with an 800×600 resolution. Once you get the Windows Vista driver for your video, you can install it and adjust video properties accordingly.

Application Compatibility Issues

Not all applications that were written for earlier versions of Windows will work with Windows Vista. After the upgrade, if you have application problems, you can address the problems as follows:

- If the application is compatible with Windows Vista, reinstall the application after the upgrade is complete.
- If the application uses Dynamic Link Libraries (DLLs), and there are migration DLLs for the application, apply the migration DLLs.

- Use the Microsoft Application Compatibility Toolkit (ACT) version 5.0 or later to determine the compatibility of your current applications with Windows Vista. ACT will determine which applications are installed, identify any applications that may be affected by Windows updates, and identify any potential compatibility problems with User Account Control and Internet Explorer. Reports can be exported for detailed analysis.
- If applications were written for earlier versions of Windows but are incompatible with Windows Vista, use the Windows Vista Program Compatibility Wizard, from Start ➢ All Programs ➢ Accessories ➢ Program Compatibility Wizard. This utility is covered in greater detail in the "Dealing with Incompatible Software Applications" section later in this chapter.
- If the application is not compatible with Windows Vista, upgrade your application to a Windows Vista–compliant version.

Windows Vista Upgrade Advisor

To assist you in the upgrade process, the Windows Vista Setup program can check the compatibility of your system, devices, and installed applications and then provide the results to you. You can then analyze these results to determine whether your hardware or software applications will port properly from Windows 2000 Professional or Windows XP to Windows Vista.

You can access the Windows Vista Upgrade Advisor web page by launching `setup.exe` on the Windows Vista media and clicking Check Compatibility Online. Alternatively, you download it from `http://www.microsoft.com/windowsvista/getready/upgradeadvisor/default.mspx`.

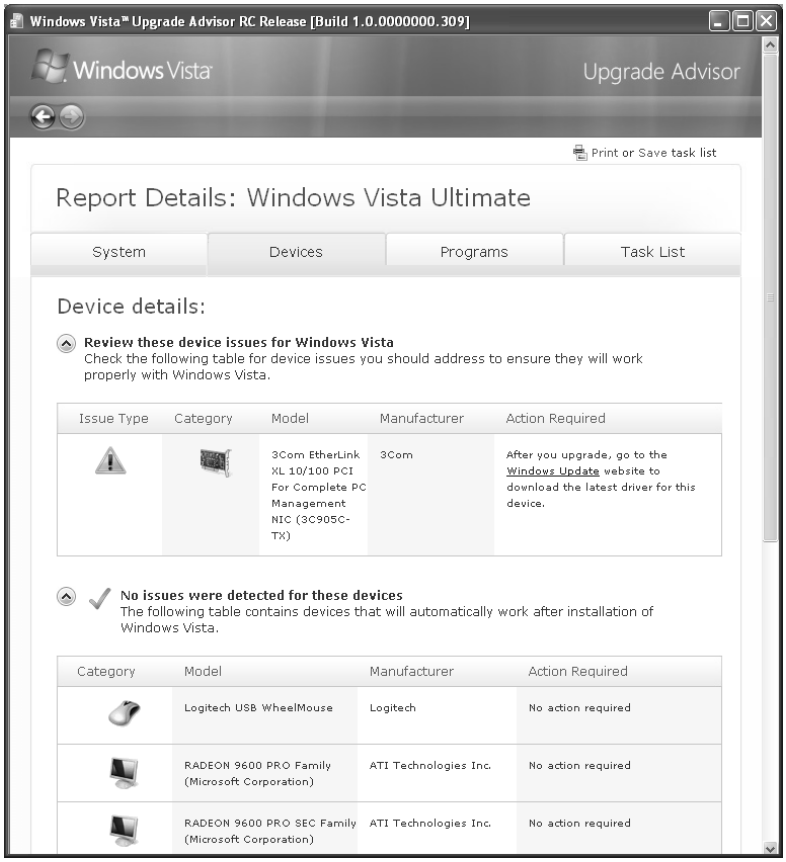
When installing the Windows Vista Upgrade Advisor, you may be prompted to download and install Microsoft Core XML Services (MSXML) 6.0 or later and .NET Framework version 2.0 or later.

After your computer is scanned, the Upgrade Advisor will determine whether any incompatibilities exist between your computer and Home Basic, Home Premium, Business, and Ultimate. It will also tell you which edition of Windows Vista seems to be best for your computer. However, you are by no means limited to upgrading to the recommended edition.

Compatibility reports are broken up into three categories:

- The System Requirements report will alert you to any shortcomings your system might have when running certain editions of Windows Vista. For example, my lab computer should have no problems accessing all the features of Windows Vista Business, but it won't be able to access all of the features of Windows Vista Home Premium or Windows Vista Ultimate because it doesn't have a TV tuner card.
- The Drivers report will alert you to any potential Windows Vista driver issues. Each device in your system will be listed in this section either as a device to be reviewed or as a device that should automatically work after Windows Vista is installed. As shown in Figure 1.1, we will need a driver for the network card after Windows Vista is installed.
- The Programs report will alert you to any potential application compatibility issues.

FIGURE 1.1 Windows Vista Upgrade Advisor



You can also save or print a task list that tells you the most compatible Windows Vista edition, your current system configuration, and the steps you need to take before and after installing Windows Vista.

An Upgrade Checklist

Once you have made the decision to upgrade, you should develop a plan of attack. The following upgrade checklist (valid for upgrading from Windows 2000 Professional and Windows XP) will help you plan and implement a successful upgrade strategy.

- Verify that your computer meets the minimum hardware requirements for Windows Vista.
- Be sure that your hardware is on the HCL.
- Make sure you have the Windows Vista drivers for the hardware. You can verify this with the hardware manufacturer.
- Run the Windows Vista Upgrade Advisor tool from the Microsoft website, which also includes documentation on using the utility, to audit the current configuration and status

of your computer. It will generate a report of any known hardware or software compatibility issues based on your configuration. You should resolve any reported issues before you upgrade to Windows Vista.

- Make sure that your BIOS is current. Windows Vista requires that your computer has the most current BIOS. If it does not, the computer may not be able to use advanced power-management features or device-configuration features. In addition, your computer may cease to function during or after the upgrade. Use caution when performing BIOS updates, as installing the incorrect BIOS can cause your computer to fail to boot.
- Take an inventory of your current configuration. This inventory should include documentation of your current network configuration, the applications that are installed, the hardware items and their configuration, the services that are running, and any profile and policy settings.
- Back up your data and configuration files. Before you make any major changes to your computer's configuration, you should back up your data and configuration files and then verify that you can successfully restore your backup. Chances are if you have a valid backup, you won't have any problems. Chances are if you *don't* have a valid backup, you will have problems.
- Delete any unnecessary files or applications, and clean up any program groups or program items you don't use. Theoretically, you want to delete all the junk on your computer before you upgrade. Think of this as the spring-cleaning step.
- Verify that there are no existing problems with your drive prior to the upgrade. Perform a disk scan, a current virus scan, and defragmentation. These, too, are spring-cleaning chores. This step just prepares your drive for the upgrade.
- Perform the upgrade. In this step, you upgrade from your previous operating system to Windows Vista.
- Verify your configuration. After Windows Vista has been installed, use the inventory to compare and test each element that was previously inventoried prior to the upgrade to verify that the upgrade was successful.

Handling an Upgrade Failure

Before you upgrade, you should have a contingency plan in place. Your plan should assume the worst-case scenario. For example, what happens if you upgrade and the computer doesn't work anymore? It is possible that, after checking your upgrade list and verifying that everything should work, your attempt at the actual upgrade may not work. If this happens, you may want to return your computer to the original, working configuration.

Indeed, we have made these plans, created our backups (two, just in case), verified our backups, and then had a failed upgrade anyway—only to discover that we had no clue where to find our original operating system CD. A day later, with the missing CD located, we were able to get up and running again. Our problem was an older BIOS, and the manufacturer of our computer did not have an updated BIOS.

Migrating Files and Settings

Rather than perform an in-place upgrade, you can choose to migrate your files and settings from an existing installation. In this case, you can use the User State Migration Tool or Windows Easy Transfer.

Windows Easy Transfer

Windows Vista ships with a utility called Windows Easy Transfer that is used to transfer files and settings from one computer to another. As shown in Figure 1.2, you can transfer some or all of the following files and settings from a computer running Windows XP with Service Pack 2 or Windows Vista:

- User accounts
- Folders and files
- Program settings
- Internet settings
- Favorites
- E-mail messages, contacts, and settings

You can use Windows Easy Transfer to migrate files from a computer running Windows 2000 with Service Pack 4, but you cannot transfer system and program settings.

FIGURE 1.2 Windows Easy Transfer

You can launch Windows Easy Transfer by inserting the Windows Vista media in your optical drive and selecting Transfer Files and Settings from Another Computer. Alternatively, you can push the wizard files to a CD or DVD, removable media, or network drive from any Windows Vista computer, and then you can launch `migwiz.exe` from the source computer.

You can launch Windows Easy Transfer from Windows Vista by selecting Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Windows Easy Transfer.

You can transfer the migrated files and settings using the following methods:

- Easy Transfer Cable, which is a USB cable that connects to the source and destination computers
- CD or DVD
- Removable media, such as a USB flash drive or a removable hard drive
- Network share
- Direct network connection

You can password-protect the migrated files and settings if you use CDs, DVDs, removable media, or a network share.

User State Migration Tool

Windows Vista ships with a utility called the *User State Migration Tool (USMT)* that is used by administrators to migrate large numbers of users over automated deployments. The USMT is similar to Windows Easy Transfer with the following differences:

- The USMT is more configurable and can use XML files to specify which files and settings are transferred.
- The USMT is scriptable and uses command-line utilities to save and restore user files and settings.

Overview of the USMT

The USMT consists of two executable files: `ScanState.exe` and `LoadState.exe`. In addition, there are three premade migration rule information files: `Migapp.xml`, `Migsys.xml`, and `Miguser.xml`. Finally, you can create a `Config.xml` file that specifies what should and should not be migrated. The purpose of these files is as follows:

- `ScanState.exe` collects user data and settings information based on the configuration of the `Migapp.xml`, `Migsys.xml`, and `Miguser.xml` files and stores it as an image file named `USMT3.mig`.
- `LoadState.exe` then deposits the information that is collected in `USMT3.mig` to a computer running a fresh copy of Windows Vista.

The information that is migrated includes the following:

- From each user:
  - My Documents
  - My Video

  - My Music
  - My Pictures
  - Desktop files
  - Start Menu
  - Quick Launch toolbar
  - Internet Explorer Favorites
- From the All Users profile:
  - Shared Documents
  - Shared Video
  - Shared Music
  - Shared Desktop files
  - Shared Pictures
  - Shared Start Menu
  - Shared Internet Explorer Favorites
- Files with certain file types, including `.doc`, `.dot`, `.rtf`, `.txt`, `.wps`, `.wri`, `.xls`, `.csv`, `.wks`, `.ppt`, `.pps`, `.pot`, `.pst`, and more
- Access Control Lists (ACLs)
- Settings for many applications, including certain versions of the following:
  - Adobe Acrobat Reader
  - Apple QuickTime Player
  - MusicMatch Jukebox Basic
  - Microsoft Windows Media Player
  - MSN Messenger
  - Microsoft Works
  - Microsoft Office
  - Quicken
  - Real Player Basic
  - WordPerfect Office
  - Yahoo Messenger
- If running Windows XP:
  - Internet Explorer settings
  - Outlook Express mail files
  - RAS settings
  - Dial-up connections

- Phone and modem options
- Accessibility settings
- Classic Desktop
- Command Prompt settings
- Wallpaper selection
- Screen saver selection
- Fonts
- Folder options
- Taskbar settings
- ODBC settings
- Mouse and keyboard settings
- Multimedia settings
- Regional settings

- If running Windows Vista:
  - Internet Explorer settings
  - Outlook Express mail files
  - RAS settings
  - Dial-up connections
  - Accessibility settings
  - Folder options
  - Taskbar settings
  - Mouse and keyboard settings
  - Multimedia settings
  - Regional settings
  - Network printers
  - Bluetooth settings
  - Media Player settings
  - FAX settings
  - IIS settings
  - Scheduled tasks
  - Terminal Server settings
  - Universal Description, Discovery, and Integration (UDDI) settings
  - Windows Logon Settings

USMT will not migrate hardware settings, drivers, passwords, application binaries, synchronization files, `.dll` files, or other executables.

Using the USMT

In its simplest form, you use the USMT in the following manner:

1. Run `ScanState.exe` on the source computer. `ScanState.exe` will copy the user state data to an intermediate store. The intermediate store (for example, a CD-RW) must be large enough to accommodate the data that will be transferred. `Scanstate.exe` would commonly be executed as a shortcut sent to users that they would deploy in the evening or through a scheduled script.
2. Install a fresh copy of Windows Vista on the target computer.
3. Run `LoadState.exe` on the target computer. `LoadState.exe` will access the intermediate store to restore the user settings.

When you use the USMT, you can create a script that can be run manually or can be used as an automated process at a scheduled time. Table 3.1 defines the options for the `Scanstate.exe` and `Loadstate.exe` commands.

TABLE 1.3 Options for *Scanstate.exe* and *Loadstate.exe*

Option	Description
`/config`	Specifies the `Config.xml` file that should be used
`/encrypt`	Encrypts the store (`Scanstate.exe` only)
`/decrypt`	Decrypts the store (`Loadstate.exe` only)
`/nocompress`	Disables data compression
`/genconfig`	Generates a `Config.xml` file but does not create a store
`/targetxp`	Optimizes ScanState for use with Windows XP
`/all`	Migrates all users
`/ue`	User exclude: excludes the specified user
`/ui`	User include: includes the specified user
`/uel`	Excludes user based on last login time
`/v` *verboselevel*	Used to identify what verbosity level will be associated with the log file on a scale of 013, with 0 being the least verbose

Installation Options

You will need to make many choices during the Windows Vista installation process. The following are some of the options that you will configure:

- How your hard disk space will be partitioned
- Windows Update and security settings
- The language and locale for the computer's settings

Before you start the installation, you should know which choices you will select. The following sections describe the options and offer considerations for picking the best ones for your installation.

Disk Space Partitioning

Disk partitioning is the act of taking the physical hard drive and creating logical partitions. A *logical drive* is how space is allocated to the drive's primary and logical partitions. For example, if you have a 200GB hard drive, you might partition it into two logical drives: a C: drive, which might be 50GB, and a D: drive, which might be 150GB.

The following are some of the major considerations for disk partitioning:

- The amount of space required
- The location of the system and boot partition
- Any special disk configurations you will use
- The utility you will use to set up the partitions

These considerations are covered in detail in the following sections.

Partition Size

One important consideration in your disk-partitioning scheme is determining the partition size. You need to consider the amount of space taken up by your operating system, the applications that will be installed, and the amount of stored data. It is also important to consider the amount of space required in the future.

Microsoft recommends that you allocate at least 20GB of disk space for Windows Vista. This allows room for the operating system files and for future growth in terms of upgrades and installation files that are placed with the operating system files.

The System and Boot Partitions

When you install Windows Vista, files will be stored in two locations: the system partition and the boot partition. The system partition and the boot partition can be the same partition.

The *system partition* contains the files needed to boot the Windows Vista operating system. The system partition contains the Master Boot Record (MBR) and boot sector of the active drive partition. It is often the first physical hard drive in the computer and normally contains the necessary files to boot the computer. The files stored on the system partition do not take any

significant disk space. The *active partition* is the system partition that is used to start your computer. The C: drive is usually the active partition.

The *boot partition* contains the files that are the Windows Vista operating system files. By default, the Windows operating system files are located in a folder named `Windows`.

Special Disk Configurations

Windows Vista supports several disk configurations. Options include simple, spanned, and striped volumes. These configuration options are covered in detail in Chapter 7, "Configuring Disks."

Windows 2000 Server and Windows Server 2003 also include options for mirrored and RAID 5 volumes.

Disk Partition Configuration Utilities

If you are partitioning your disk prior to installation, you can use several utilities, such as the DOS or Windows FDISK program or a third-party utility such as Norton's Partition Magic. You might want to create only the first partition where Windows Vista will be installed. You can then use the Disk Management utility in Windows Vista to create any other partitions you need. The Windows Vista Disk Management utility is covered in Chapter 7.

You can get more information about FDISK and other disk utilities from your DOS or Windows documentation. Also, basic DOS functions are covered in *MCSA/MCSE 2003 JumpStart: Computer and Network Basics* by Lisa Donald (Sybex, 2003).

Language and Locale

Language and locale settings determine the language the computer will use. Windows Vista supports many languages for the operating system interface and utilities.

Locale settings configure the locality for items such as numbers, currencies, times, and dates. An example of a locality is that English for United States specifies a short date as *mm/dd/yyyy* (month/day/year), while English for South Africa specifies a short date as *yyyy/mm/dd* (year/month/day).

Installing Windows Vista

You can install Windows Vista either from the bootable DVD or through a network installation using files that have been copied to a network share point. You can also launch the `setup.exe` file from within Windows 2000, Windows XP, or Windows Vista to upgrade your operating system.

The Windows Vista DVD is bootable. To start the installation, you simply restart your computer and boot to the DVD. The installation process will begin automatically.

We will discuss how to install Windows Vista in more detail in the next section.

If you are installing Windows Vista from the network, you need a *distribution server* and a computer with a network connection. A distribution server is a server that has the Windows Vista distribution files copied to a shared folder. The following steps are used to install Windows Vista over the network:

1. Boot the target computer.
2. Attach to the distribution server and access the share that has the files copied to it.
3. Launch `setup.exe`.
4. Complete the Windows Vista installation using either the clean install method or the upgrade method. These methods are discussed in detail in the following sections.

You can also install Windows Vista through an unattended process, which is covered in detail in Chapter 2, "Automating the Windows Vista Installation."

Performing a Clean Install of Windows Vista

This section describes how to perform a clean install of Windows Vista. As explained in the previous section, you can run the installation from the optical media or over a network. The only difference in the installation procedure is your starting point: from your optical drive or from a network share. The steps in the following sections assume you are using the Windows Vista DVD to install Windows Vista.

There are three main steps in the Windows Vista installation process:

1. Collecting Information
2. Installing Windows
3. Set Up Windows

We cover each of these steps in detail in the following sections.

The following sections give the details of the installation process to show how the process works. But you should not actually install Windows Vista until you reach Exercise 1.1. In that exercise, you'll set up your computer to complete the rest of the exercises in this book.

Clean Install: Collecting Information

When you boot to the Windows Vista installation media, the Setup program will automatically start the Windows Vista installation. In the Collecting Information stage of the installation, you will select your language and locale settings, enter your product key, accept the license terms, select the type of installation, and specify the install location.

The following steps are involved in a clean installation of Windows Vista (click Next after completing each step):

1. Insert the Windows Vista DVD in your computer. Restart the computer, and boot to the DVD drive. Alternatively, you can run `setup.exe` from the Windows Vista media or a network share. However, for this walk-through, we will explain how to boot to the Windows Vista DVD.
2. The Setup program will start automatically and begin loading files. At this point, the computer is running the Windows Preinstallation Environment (WinPE) operating system.

You can access the command line from within WinPE by pressing Shift+F10.

3. The Install Windows dialog box will appear. You can select the language to install, the time and currency format, and the keyboard or input method.
4. The Install Now button will appear in the center of the screen. In addition, two options will be available in the lower-left corner: What to Know Before Installing Windows, and Repair Your Computer.
5. You will be prompted to type your 25-character product key for activation. You can find the product key on a sticker on your computer or on the installation disc folder. Unlike previous versions of Windows, the product key is one long text box rather than five separate text boxes. As you type the 25-character product key, the dashes will be added for you automatically. There is also a check box to automatically activate Windows when online.
6. The Microsoft Windows Vista license terms will appear. The installation will not allow you to click Next until you have accepted the license terms.
7. You will be prompted to select the type of installation you want to perform. A Custom installation will install a clean copy of Windows Vista and will also allow you to select the installation location or make changes to disks and partitions. This option is also required for multiboot installations.

The option for performing an Upgrade installation will be unavailable to you. To upgrade, you must start the installation from within Windows.

8. You will be prompted for the location where you want to install Windows Vista. This will list all existing disks and partitions on your computer. To add, delete, format, or extend a partition, select the Drive Options (advanced) option.
9. If an existing installation of Windows is located on the partition you selected, a dialog box will appear warning you that files and folders from your existing installation will be moved to a directory named `Windows.old`.

If Windows Vista does not recognize your hard drive controller or hard drive because it uses a driver that is not on the Windows Vista DVD, you will need to select the Load Driver option and load the driver from a floppy disk, CD, DVD, or USB flash drive.

Clean Install: Installing Windows

During the Installing Windows phase, all the files required by the Setup program will be copied to the hard drive. During the process, the computer automatically reboots during the installation process. This process will take several minutes and will proceed automatically without user intervention.

The following steps are displayed on the screen along with a completion percentage for each:

1. Copying Windows Files
2. Expanding Files
3. Installing Features
4. Installing Updates
5. Completing Installation

During the installation process, you may see your screen flicker as the video driver is detected.

Clean Install: Set Up Windows

Once your computer finishes copying files and reboots, you will be in the Set Up Windows phase of the installation. In this final stage, you will configure a user account, specify a computer name, select update and feature settings, and configure the time and date.

The following steps are involved (click Next after completing each step):

1. You will be prompted to choose a username, password, password hint, and picture.
2. You will be prompted to type a computer name that will uniquely identify your computer on the network. The installation program suggests a name, but you can change it to another name. Your computer name can be up to 15 characters. You can also select your desktop background.

Be sure that the computer name is a unique name within your network. If you are part of a corporate network, you should also verify that the computer name follows the naming convention specified by your Information Services (IS) department.

3. Settings related to Windows Update and security will appear. You can use the recommended settings, install important updates for Windows only, or have the computer ask you later. If you select the option to use the recommended settings, the following settings will be configured:
   - Windows Update will be enabled and updates will automatically install.
   - Windows Defender will be installed and any collected information will be sent to Microsoft.
   - Errors will automatically be sent to Microsoft.
   - The latest drivers for your hardware will automatically be downloaded from Windows Update.
   - The Internet Explorer Phishing Filter will be enabled.
4. Options related to the date, time, and time zone will appear.
5. The installation program will thank you, and a Start button will appear in the lower-right corner.
6. Windows will check your computer's performance.
7. The username that was configured will be displayed and you will be prompted for a password. This is the standard Windows Vista login screen.

You should make a complete backup of your computer before repartitioning your disk or installing new operating systems. All data will be lost during this process!

Setting Up Your Computer for Hands-On Exercises

Before beginning Exercise 1.1, verify that your computer meets the requirements for installing Windows Vista as listed in Table 1.1. Exercise 1.1 assumes you are not currently running a previous version of Windows that will be upgraded.

The exercises in this book assume that your computer is configured in a specific manner. Your computer should have at least a 20GB drive that is configured with the minimum space requirements and partitions. Other exercises in this book assume that your computer is configured as follows:

- 20GB C: partition with the NTFS file system

- Optional D: partition with the NTFS file system
- 1GB or more of unallocated space

Of course, you can allocate more space to your partitions if it is available.

You are probably wondering about the free space requirement. You need free space because you will create a new volume in Chapter 7. If no free space exists, you won't be able to complete that exercise.

As noted earlier in this chapter, you can set up your partitions by using the Windows Vista installation utility, the DOS or Windows FDISK utility, or a third-party program. For example, if you have a Windows 98 computer, you can use it to create a Windows 98 boot disk. Then, copy FDISK from the `Windows` folder on the Windows 98 computer to the boot disk.

In Exercise 1.1, you will be installing a clean install of Windows Vista on your system.

You can use Windows Easy Transfer to migrate your user account information, files and folders, program settings, Internet settings, Favorites, and e-mail configuration settings. See the section in this chapter covering Windows Easy Transfer.

If you want to perform an upgrade install of Windows Vista, follow the steps in Exercise 1.2.

EXERCISE 1.1

Performing a Clean Install of Windows Vista

In this exercise, you will perform a clean install of Windows Vista. This exercise assumes that you have access to Windows Vista Ultimate; other editions may vary slightly.

Collecting Information

1. Boot your computer with the Windows Vista media inserted into your optical drive.
2. After the computer loads the required files, the Install Windows dialog box will appear. Ensure these settings are correct and click the Next button.
3. In the next dialog box, click the Install Now button to continue.
4. Type your 25-digit product key, and click Next to continue.
5. Click the check box I Accept the License Terms, and click Next to continue.

EXERCISE 1.1 *(continued)*

6. Click Custom to install a clean copy of Windows.
7. Select the partition where you want to install Windows Vista, and click Next. If you do not have an existing partition that is adequate for Windows Vista installation, select Drive Options (advanced) and create, delete, or extend partitions as necessary. It is not necessary to format the partition before continuing.
8. If an existing version of Windows is located on the partition you selected, a dialog box will appear warning you that files and folders from your existing installation will be moved to `Windows.old`. Click OK to continue.

Installing Windows

1. The Installing Windows phase of installation will begin. No intervention is required during this phase.

Set Up Windows

1. Enter a username and a password. You will be required to enter the password twice. If you want, you can also enter a password hint in case you forget your password. Select a picture for your user account, and click Next to continue.
2. Enter a computer name, select a desktop background, and click Next to continue.
3. Settings related to Windows Update and security will appear. For this walk-through, click Use Recommended Settings.
4. Settings related to the date and time will appear. Ensure that the date, time, and time zone settings are correct, and click Next to continue.
5. The Thank You dialog box will appear. Click the Start button to continue. Windows will check your computer's performance while informational icons appear.

Windows Vista is now installed, and you will be prompted to log in with your new username and password.

Performing an Upgrade to Windows Vista

This section describes how to perform an upgrade to Windows Vista. Similar to a clean install, you can run the installation from the optical media or over a network. The only difference in the installation procedure is your starting point: from your optical drive or from a network share. The steps in the following sections assume that you are using the Windows Vista DVD to install Windows Vista.

There are three main steps in the Windows Vista upgrade process:

1. Collecting Information

2. Upgrading Windows
3. Set Up Windows

We will cover each of these steps in detail in the following sections.

The following sections give the details of the installation process to show how the process works. But you should not actually upgrade Windows Vista until you reach Exercise 1.2. In that exercise, you'll set up your computer to complete the rest of the exercises in this book.

Upgrade: Collecting Information

The Collecting Information stage of the upgrade is slightly different from a clean installation. The following steps are involved with an upgrade installation (click Next after completing each step):

1. Insert the Windows Vista DVD in your computer, and run `setup.exe` from the Windows Vista media. Alternatively, you can run `setup.exe` from a network share.

If you boot the computer to the Windows Vista DVD, you will only have the option to perform a clean install.

2. You will be presented with the Windows Vista installation dialog box, as shown in Figure 1.3. From here, you can choose to install Windows Vista, check the compatibility of your system online by using the Windows Vista Upgrade Advisor, read about the Windows installation process, and transfer files and settings from another computer by using Windows Easy Transfer.

We discussed Windows Vista Upgrade Advisor and Windows Easy Transfer earlier in this chapter.

3. You will be prompted to update your current operating system. If you choose not to update, the installation might fail. You can also choose to send information to Microsoft during this process.
4. You will be prompted to type your 25-character product key for activation. You can find the product key on a sticker on your computer or on the installation disc folder. Unlike previous versions of Windows, the product key is one long text box rather than five separate text boxes. As you type the 25-character product key, the dashes will be added for you automatically. There is also a check box to automatically activate Windows when online.
5. The Microsoft Windows Vista license terms will appear. The installation will not allow you to click Next until you have accepted the license terms.

FIGURE 1.3 Windows Vista installation screen

6. You will be prompted to select the type of installation you want to perform. An Upgrade installation can be performed only if you have an operating system that can be upgraded to Windows Vista. In order to upgrade, you must start the installation from within Windows.

The Custom option is required for multiboot installations.

7. You will see a compatibility report that will alert you of any applications or drivers that are not supported in Windows Vista.

You can right-click and select Print from the context menu if you want to print the compatibility report.

Upgrade: Upgrading Windows

During the Upgrading Windows phase, all the files required by the Setup program will be copied to the hard drive. During the process, the computer automatically reboots during the installation process. This process will take several minutes and will proceed automatically without user intervention.

The following steps appear on the screen along with a completion percentage for each:

1. Copying Windows Files
2. Gathering Files
3. Expanding Files
4. Installing Features and Updates
5. Completing Upgrade

During the installation process, you may see your screen flicker as the video driver is detected.

Upgrade: Set Up Windows

Once your computer finishes copying files and reboots, you will be in the Set Up Windows phase of the installation. The following steps are involved with an upgrade installation (click Next after completing each step):

1. You can select the country, the time and currency format, and the keyboard layout.
2. Settings related to Windows Update and security will appear. You can use the recommended settings, install important updates for Windows only, or have the computer ask you later. If you select the option to use the recommended settings, the following settings will be configured:
   - Windows Update will be enabled and updates will automatically install.
   - Windows Defender will be installed and any collected information will be sent to Microsoft.
   - Errors will automatically be sent to Microsoft.
   - The latest drivers for your hardware will automatically be downloaded from Windows Update.
   - The Internet Explorer Phishing Filter will be enabled.
3. Options related to the date, time, and time zone will appear.
4. Windows will check your computer's performance.
5. Installation will complete and you will be allowed to log in to Windows Vista.

In Exercise 1.2, you will be performing an upgrade install of Windows Vista on your system.

You should make a complete backup of your computer before repartitioning your disk or installing new operating systems. All data will be lost during this process!

You can use Windows Easy Transfer to migrate your user account information, files and folders, program settings, Internet settings, Favorites, and e-mail configuration settings. See the section in this chapter covering Windows Easy Transfer.

If you want to perform a clean install of Windows Vista, follow the steps in Exercise 1.1.

EXERCISE 1.2

Performing an Upgrade Install of Windows Vista

In this exercise, you will perform an upgrade install of Windows Vista. This exercise assumes that you are upgrading Windows XP Professional to Windows Vista Ultimate; other editions may vary slightly.

Collecting Information

1. Insert the Windows Vista media into your optical drive. If Autoplay is enabled, you will see the Windows Vista installation dialog box. If not, launch `setup.exe` from the Windows Vista media.
2. The Windows Vista installation dialog box will appear. Click Install Now to continue.
3. In the next dialog box, select the option to upgrade your computer if your computer is not up-to-date.
4. Type your 25-digit product key and click Next to continue.
5. Click the check box I Accept the License Terms, and click Next to continue.
6. Click Upgrade to upgrade your version of Windows.
7. Read the compatibility report, and click Next.

Upgrading Windows

1. The Upgrading Windows phase of installation will begin. No intervention is required during this phase.

Set Up Windows

1. Ensure the correct country, time and currency, and keyboard layout settings are selected, and then click Next to continue.

EXERCISE 1.2 *(continued)*

2. Settings related to Windows Update and security will appear. For this walk-through, click Use Recommended Settings.
3. Settings related to the date and time will appear. Ensure that the date, time, and time zone settings are correct, and click Next to continue.
4. Windows will check your computer's performance while informational icons appear.

Windows Vista is now installed, and you will be prompted to log in with your existing username and password.

Using Windows Anytime Upgrade

You can also upgrade Windows Vista Home Basic, Home Premium or Business to a more advanced edition of Vista through Windows Anytime Upgrade. You can upgrade the following editions:

- Home Basic users can upgrade to Home Premium or Ultimate.
- Home Premium users can upgrade to Ultimate.
- Business users can upgrade to Ultimate.

To access Windows Anytime Upgrade, select Start ➢ Control Panel ➢ System and Maintenance ➢ Windows Anytime Upgrade. After selecting the upgrade you want to perform, you can purchase a license from a Microsoft partner, download and install the license, and install the additional features from the Windows Vista media.

Troubleshooting Installation Problems

The Windows Vista installation process is designed to be as simple as possible. The chances for installation errors are greatly minimized through the use of wizards and the step-by-step process. However, it is possible that errors may occur.

In the next sections, you will learn more about the following:

- Identifying and resolving common installation problems
- Installing nonsupported hard drives
- Troubleshooting installation errors using installation log files

Identifying Common Installation Problems

As most of you are aware, installations seldom go off without a hitch. Table 1.3 lists some possible installation errors you might encounter.

TABLE 1.4 Common Installation Problems

Problem	Description
Media errors	Media errors are caused by defective or damaged CDs or DVDs. To check the disc, put it into another computer and see if you can read it. Also check your disc for scratches or dirt—it may just need to be cleaned.
Insufficient disk space	Windows Vista needs at least 15GB of free space for the installation program to run properly. If the Setup program cannot verify that this space exists, the program will not let you continue.
Not enough memory	Make sure that your computer has the minimum amount of memory required by Windows Vista (512MB). Having insufficient memory may cause the installation to fail or blue-screen errors to occur after installation.
Not enough processing power	Make sure that your computer has the minimum processing power required by Windows Vista (800MHz). Having insufficient processing power may cause the installation to fail or blue-screen errors to occur after installation.
Hardware that is not on the HCL	If your hardware is not listed on the HCL, Windows Vista may not recognize the hardware or the device may not work properly.
Hardware with no driver support	Windows Vista will not recognize hardware without driver support.
Hardware that is not configured properly	If your hardware is Plug and Play–compatible, Windows should configure it automatically. If your hardware is not Plug and Play–compatible, you will need to manually configure the hardware per the manufacturer's instructions.
Incorrect product key	Without a valid product key, the installation will not go past the Product Key screen. Make sure that you have not typed in an incorrect key (check your Windows Vista installation folder or your computer case for this key).
Failure to access TCP/IP network resources	If you install Windows Vista with typical settings, the computer is configured as a DHCP client. If there is no DHCP server to provide IP configuration information, the client will still generate an autoconfigured IP address but be unable to access network resources through TCP/IP if the other network clients are using DHCP addresses.

Installing Nonsupported Hard Drives

If your computer is using a hard disk that does not have a driver included on the Windows Vista media, you will receive an error message stating that the hard drive cannot be found. You should verify that the hard drive is properly connected and functional. You will need to obtain a disk driver from the manufacturer for Windows Vista and then specify the driver location by selecting the Load Driver option during partition selection.

Dealing with Incompatible Software Applications

You may have legacy applications that will not run under Windows Vista. Microsoft provides a Program Compatibility Wizard to help address this issue. You should not use this wizard if the application makes kernel-level calls or if the application is Windows Vista–compatible. To use the wizard, perform the following steps:

1. Select Start ➢ All Programs ➢ Accessories ➢ Program Compatibility Wizard.
2. You will see a caution statement that this wizard should not be used for older virus detection, backup, or system programs. Click the Next button.
3. Locate the program that requires the compatibility settings. Choose from the options that appear on your screen, and click the Next button:
   - Select from a list of programs (Windows Vista will detect all currently installed programs and provide you with a list).
   - Use the program in the CD-ROM drive.
   - Locate the program manually.
4. The next option allows you to select the compatibility for the application. Choose from the options that appear on your screen and click the Next button:
   - Microsoft Windows 95
   - Microsoft Windows NT 4.0 (Service Pack 5)
   - Microsoft Windows 98/Windows Me
   - Microsoft Windows 2000
   - Microsoft Windows XP (Service Pack 2)
   - Do not apply a compatibility mode
5. The next option allows you to configure the display settings for the program. Choose from the options that appear on your screen, and click the Next button:
   - 256 Colors
   - 640×480 Screen Resolution
   - Disable Visual Themes
   - Disable Desktop Composition
   - Disable Display Scaling on High DPI Settings

6. You will be asked whether the program requires administrator privileges. If required, click the check box to run the program as an administrator, and then click the Next button.
7. You will then be asked to confirm your selections. After you click Next, a test will be performed to verify that the settings work with your application.
8. You will be asked whether the program worked correctly. You can choose from the following answers:
   - Yes, Use These Settings
   - No, Try Different Settings
   - No, But I Am Finished Trying Settings
9. Microsoft will want you to send them information about your compatibility settings. Choose whether you want to send the information to Microsoft, and then select Next. Click Finish to exit the wizard.

The most common applications that require you to change video settings are older educational software programs and games.

Troubleshooting with Installation Log Files

When you install Windows Vista, the Setup program creates several log files. You can view these logs to check for any problems during the installation process. Two log files are particularly useful for troubleshooting:

- The action log includes all of the actions that were performed during the setup process and a description of each action. These actions are listed in chronological order. The action log is stored as `\Windows\setupact.log`.
- The error log includes any errors that occurred during the installation. For each error, there is a description and an indication of the severity of the error. This error log is stored as `\Windows\setuperr.log`.

In Exercise 1.3, you will view the Windows Vista setup logs to determine whether there were any problems with your Windows Vista installation.

EXERCISE 1.3

Troubleshooting Failed Installations with Setup Logs

In this exercise, you will view the installation with setup logs, which could be helpful in troubleshooting failed installations.

1. Select Start ➢ Computer.
2. Double-click Local Disk (C:).

EXERCISE 1.3 *(continued)*

3. Double-click Windows.
4. In the `Windows` folder, double-click the `setupact` file to view your action log in Notepad. When you are finished viewing this file, close Notepad.
5. Double-click the `setuperr` file to view your error file in Notepad. If no errors occurred during installation, this file will be empty. When you are finished viewing this file, close Notepad.
6. Close the directory window.

Supporting Multiple-Boot Options

You may want to install Windows Vista but still be able to run other operating systems. *Dual-booting* or *multibooting* allows your computer to boot multiple operating systems. Your computer will be automatically configured for dual-booting if there was a supported operating system on your computer prior to the Windows Vista installation, you didn't upgrade from that operating system, and you installed Windows Vista into a different partition.

One reason for dual-booting is to test various systems. If you have a limited number of computers in your test lab and you want to be able to test multiple configurations, you dual-boot. For example, you might configure one computer to multiboot with Windows 2000 Professional, Windows XP Professional, and Windows Vista.

Another reason to set up dual-booting is for software backward compatibility. For example, you may have an application that works with Windows 98 but not under Windows Vista. If you want to use Windows Vista but still access your legacy application, you can configure a dual-boot.

Here are some keys to successful dual-boot configurations:

- Make sure you have plenty of disk space.
- Windows Vista must be installed on a separate partition in order to dual-boot with other operating systems.
- Install older operating systems before installing newer operating systems. If you want to support dual-booting with DOS and Windows Vista, DOS must be installed first. If you install Windows Vista first, you cannot install DOS without ruining your Windows Vista configuration. This requirement also applies to Windows 9*x*, Windows 2000, and Windows XP.
- Never, ever upgrade to Windows Vista dynamic disks. Dynamic disks are seen only by Windows 2000, Windows XP Professional, Windows Server 2003, and Windows Vista, and are not recognized by any other operating system, including Windows NT and Windows XP Home Edition.
- Only Windows NT 4.0 (with Service Pack 4), Windows 2000, Windows XP, and Windows Server 2003 can recognize NTFS file systems. Other Windows operating systems

use FAT16 or FAT32 and cannot recognize NTFS. All Windows-based operating systems can recognize FAT partitions.

- If you will dual-boot with Windows 9*x*, you must turn off disk compression or Windows Vista will not be able to read the drive properly.
- Do not install Windows Vista on a compressed volume unless the volume was compressed using NTFS compression.
- Files that are encrypted with Windows Vista will not be available to Windows NT 4.

If you are planning on dual-booting with Windows NT 4, you should upgrade it to NT 4 Service Pack 4 (or higher), which provides NTFS version 5 support.

Once you have installed each operating system, you can choose the operating system that you will boot to during the boot process. You will see a boot selection screen that asks you to choose which operating system you want to boot.

The Boot Configuration Data (BCD) store contains boot information parameters that were previously found in `boot.ini` in older versions of Windows. To edit the boot options in the BCD store, use the BCDEdit utility, which can be launched only from a command prompt. To open a command prompt window, you can do the following:

1. Launch `\Windows\system32\cmd.exe`.
2. Open the Run command by pressing Windows+R and then entering **cmd**.
3. Open Run from the Start menu, if the Start menu is configured to display it.

After the command prompt windows is open, type **bcdedit** to launch BCDEdit.

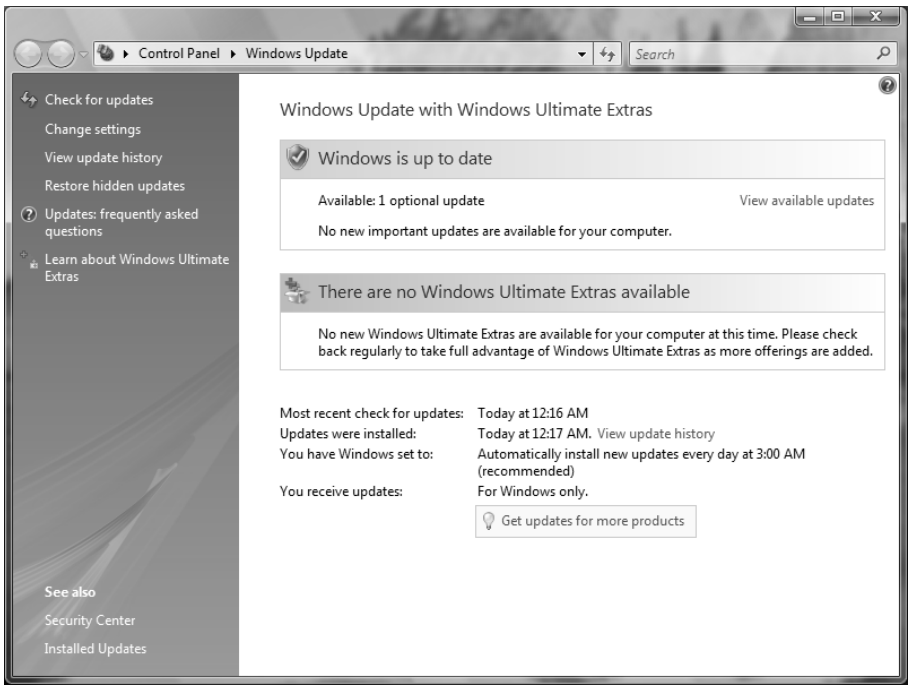
Using Windows Activation

Windows Activation is Microsoft's way of reducing software piracy. Unless you have a corporate license for Windows Vista, you will need to perform postinstallation activation. This can be done online or through a telephone call. Windows Vista will attempt automatic activation three days after you log on to Windows Vista for the first time. There is a 30-day grace period when you will be able to use the operating system without activation. After the grace period expires, you will not be able to create new files or save changes to existing files until Windows Vista is activated. When the grace period runs out, the Windows Activation Wizard will automatically start; it will walk you through the activation process.

Using Windows Update

Windows Update, as shown in Figure 1.4, is a utility that connects to Microsoft's website and checks to ensure that you have the most up-to-date version of Microsoft products.

FIGURE 1.4 Windows Update



Some of the common update categories associated with Windows Update are as follows:

- Critical updates
- Service packs
- Drivers

Follow these steps to configure Windows Update:

1. Select Start ➢ Control Panel.
   - From Windows Classic View, select Windows Update.
   - From Windows Category View, select System and Maintenance ➢ Windows Update.
2. Configure the options you want to use for Windows Update, and click OK.

The options you can access from Windows Update include the following:

- Check for Updates
- Change Settings
- View Update History
- Restore Hidden Updates
- Updates: Frequently Asked Questions

- Learn About Windows Ultimate Extras
- Security Center
- Installed Updates
- Get Updates for More Products

We will cover all these options in detail in the following sections.

Check for Updates

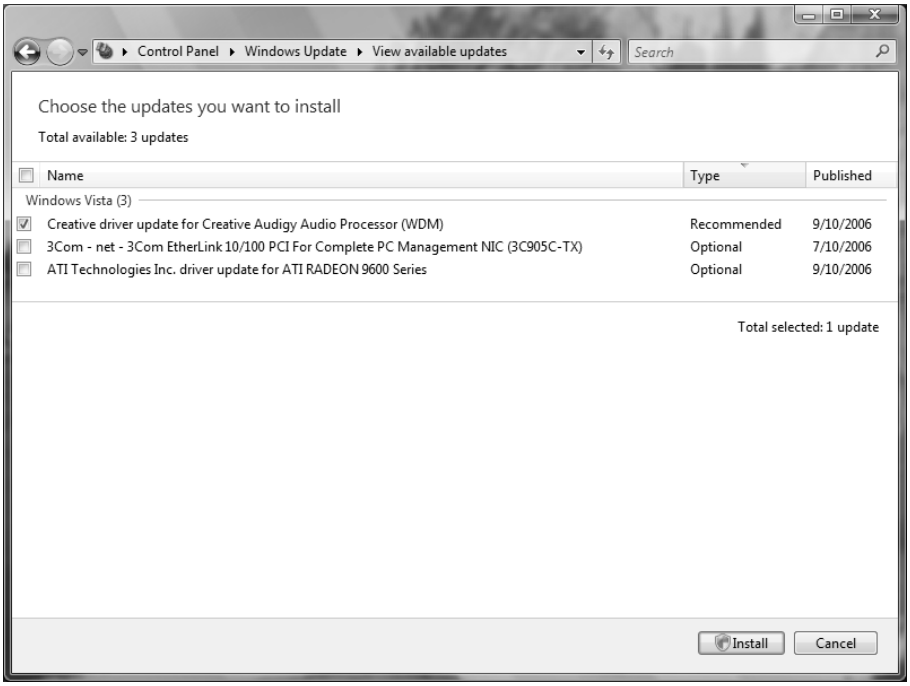
When you click Check for Updates, Windows Update will retrieve a list of available updates from the Internet. You can then click View Available Updates to see what updates are available. Updates are marked as Important, Recommended, or Optional. Figure 1.5 shows a sample list of updates.

Change Settings

Clicking Change Settings allows you to customize how Windows can install updates. You can configure the following options:

- The frequency and time that updates will be downloaded to your computer

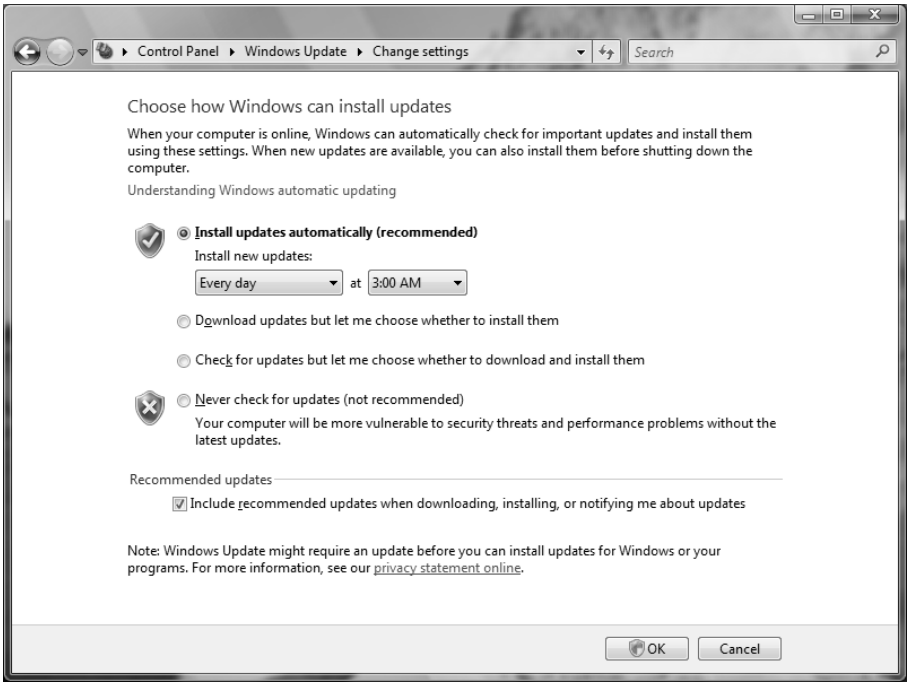
FIGURE 1.5 Windows Update sample list of updates



- Whether updates will be downloaded and if you want to choose to install them
- Whether you want to be notified that updates are available, but not to download or install them
- Disable checking for updates

Figure 1.6 shows the settings that can be configured for Windows Update.

FIGURE 1.6 Windows Update, Change Settings

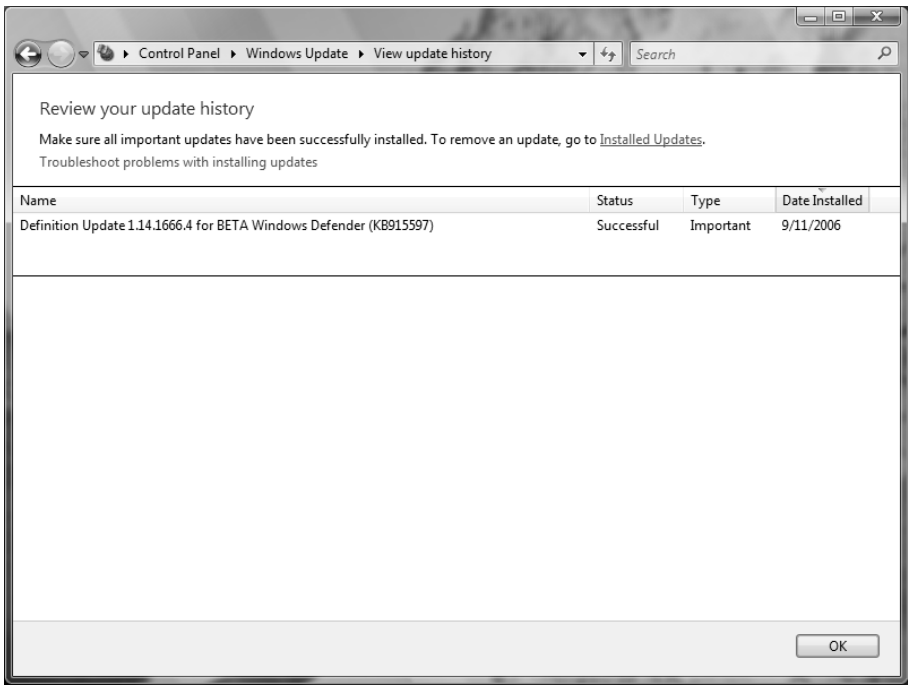


View Update History

View Update History, as shown in Figure 1.7, is used to view a list of all of the installations that have been performed on the computer. You can see the following information for each installation:

- Update Name
- Status (Successful, Unsuccessful, or Canceled)
- Type (Important, Recommended, or Optional)
- Date Installed

FIGURE 1.7 Windows Update, View Update History



Restore Hidden Updates

With Restore Hidden Updates you can list any updates that you have hidden from the list of available updates. An administrator might hide updates that they do not want users to install.

Update: Frequently Asked Questions

With Update: Frequently Asked Questions, you can launch Help and Support to answer frequently asked questions about Windows Update.

Learn About Windows Ultimate Extras

Learn About Windows Ultimate Extras, as you might imagine, appears only in Windows Vista Ultimate, and it discusses those features that are available only with Windows Vista Ultimate.

Security Center

Clicking Security Center opens the Windows Security Center, which allows you to see the status of your firewall, automatic update settings, malware protection, and other security settings.

We will discuss Windows Security Center in more detail in Chapter 6, "Configuring Security."

Installed Updates

Installed Updates allows you to see the updates that are installed and to uninstall or change them if necessary. The Installed Updates feature is a part of the Programs and Features applet in Control Panel, which allows you to uninstall, change, and repair programs.

Get Updates for More Products

Clicking this link will direct you to a website to download Microsoft Update, which can be used not only to update Windows Vista but also to update other Microsoft products, such as Microsoft Office.

Installing Windows Service Packs

Service packs are updates to the Windows Vista operating system that include bug fixes and product enhancements. Some of the options that might be included in service packs are security fixes or updated versions of software, such as Internet Explorer.

Prior to installing a service pack, you should perform the following steps:

1. Back up your computer.
2. Check your computer to ensure that it is not running any malware or other unwanted software.
3. Check with your computer manufacturer to see whether there are any special instructions for your computer prior to installing the service pack.

You can download service packs from `Microsoft.com`, you can receive service packs via Windows Update, or you can pay for a copy of the service pack to be mailed to you on disc. Before you install a service pack, you should read the Release Note that is provided for each service pack on Microsoft's website.

Summary

In this chapter, you learned how to install and upgrade Windows Vista. We covered the following topics:

- Installation preparation, which begins with making sure that your computer meets the minimum system requirements and that all of your hardware is on the Hardware Compatibility List (HCL). Then you need to decide whether you will perform a clean install or

an upgrade. Finally, you should plan which options you will select during installation. Options include methods of partitioning your disk space, your username and password, and whether you want to enable Windows Update and other security features.

- The methods you can use for installation, which include using the distribution files on the Windows Vista media or using files that have been copied to a network share point.
- The client upgrade paths that can upgrade to Windows Vista and the minimum hardware requirements to perform an upgrade.
- Guidelines for when you should upgrade and when you should perform a clean install of Windows Vista.
- Upgrade considerations and potential problems with the Windows Vista upgrade process.
- An upgrade checklist with steps to help ensure a successful upgrade.
- How to migrate files and settings from one computer to another using Windows Easy Transfer and how to migrate user data from one computer to another using the User State Migration Tool.
- How to install Windows Vista.
- How to upgrade Windows Vista.
- How to troubleshoot and resolve common installation errors.
- How to troubleshoot installation problems. Common errors are caused by media problems, lack of disk space or memory, and hardware problems. Other common errors include using nonsupported hard drives. You can view setup log files to check for problems that occurred during the installation.
- How to resolve application compatibility issues.
- Information about supporting dual-boot or multiboot environments. Dual-booting and multibooting allow you to boot to a choice of two or more operating systems.
- The Windows Update and Windows Activation features. Postinstallation updates are used to ensure that you have the latest files. Product activation is used to complete the Windows Vista licensing process.

Exam Essentials

Be able to tell whether a computer meets the minimum hardware requirements for Windows Vista. Windows Vista has minimum hardware requirements that must be met. In addition, the hardware must be listed on the HCL, and Windows Vista drivers must be available for all devices.

Understand the different methods that can be used for Windows Vista installation. Be able to specify the steps and setup involved in installing Windows Vista through options such as optical media and network installation.

Understand how to migrate users from one computer to another computer. Know how to use Windows Easy Transfer and the User State Migration Tool.

Understand the reasons why a Windows Vista installation might fail. You should be able to list common reasons for failure of a Windows Vista installation and be able to offer possible fixes or solutions.

Specify what is required to support multiple-boot configurations. If you plan to install Windows Vista on the same computer that is running other operating systems, be able to specify what must be configured to support dual- or multiple-boot configurations.

Be able to list the requirements for a Windows Vista upgrade. Know the requirements for upgrading a computer to Windows Vista, including which operating systems can be upgraded, what the hardware requirements are, and the steps for completing an upgrade.

Know all the possible issues that may arise during a Windows Vista upgrade. Be aware of possible upgrade problems, including application compatibility problems. Know how to use the Program Compatibility Wizard.

Review Questions

1. James is the network administrator for a large corporation. He is in charge of compatibility testing and needs to test his corporation's standard applications on the Windows Vista operating system. He has decided to install Windows Vista on a test computer in the lab. He can choose among several computers. When making his selection, what is the minimum processor required for an Intel-based computer to install and run Windows Vista?

   A. A Celeron or Pentium III with a 600MHz or better processor

   B. A Celeron or Pentium III with a 800MHz or better processor

   C. A Celeron or Pentium III with a 1GHz or better processor

   D. A Celeron or Pentium 4 with a 1.6GHz or better processor

2. Martina has Windows 2000 Professional installed on her home desktop computer. This computer is running some applications that require the use of her sound card; however, her sound card does not have a Windows Vista–compatible driver. Martina is planning on replacing the sound card at some point, and she has purchased an upgrade to Windows Vista. She decides to install Windows Vista on her desktop computer in a dual-boot configuration. She has an extra 30GB partition that can be used. What is the minimum free disk space required to install Windows Vista on the extra partition?

   A. 1GB

   B. 5GB

   C. 15GB

   D. 20GB

3. Dionne has 12 identical computers in the training room. She wants to upgrade them to Windows Vista, but before she does, she wants to ensure that the hardware is compatible. What can be used to determine whether the computers' hardware components are supported by Windows Vista? (Choose all that apply.)

   A. Windows Vista Upgrade Advisor

   B. Windows Vista Help and Support

   C. The Microsoft Compatibility List

   D. The Hardware Compatibility List

4. You are the network administrator for a small company. You have recently purchased 20 brand-new computers that came with no operating system but are configured with the latest hardware. Each computer has a SCSI controller and an 80GB SCSI hard drive. You put the Windows Vista DVD in the DVD drive and start the installation. During the partition configuration phase, the disk is not displayed. You do not see any partitions available, nor do you see any unallocated space. Which of the following actions should you take?

   A. Install a full version of Windows XP Professional on the computer, and then upgrade to Windows Vista.

   B. Verify that the BIOS for the SCSI controller is enabled.

   C. Click Load Driver and provide the Windows Vista device drivers that are on the manufacturer's CD or downloaded from the manufacturer's website.

   D. Replace the SCSI drive with a drive that has a driver on the Windows Vista DVD.

5. Josh is the network administrator of a large company. The company's computers run a variety of Windows operating systems, including Windows 2000 Professional, Windows XP Professional, Windows XP Professional *x*64, and Windows XP Tablet PC. Josh wants to upgrade all of the computers to Windows Vista Business. Which of the following operating systems require a clean install? (Choose all that apply.)

   A. Windows 2000 Professional

   B. Windows XP Professional

   C. Windows XP Professional *x*64

   D. Windows XP Tablet PC

6. Vince runs a home-based business using two Windows XP Professional computers. The XP Professional computers are installed with many applications and configured so that he can use them efficiently. He asks you for advice regarding upgrading his operating systems to Windows Vista, but he wants to ensure that his applications and settings will remain intact. Which Windows Vista operating systems can Vince upgrade by performing an in-place upgrade? (Choose all that apply.)

   A. Windows Vista Home Basic

   B. Windows Vista Home Premium

   C. Windows Vista Business

   D. Windows Vista Ultimate

7. Adam performed a clean installation of Windows Vista on his Windows XP Professional computer. However, he chose to install Windows Vista in the same partition as his Windows XP Professional installation. He asks you if there's any way to retrieve his old files. In which directory would you tell Adam that his files for his old operating system are stored?

   A. `\Windows`

   B. `\Windows.old`

   C. `\Windows\old`

   D. `\WindowsXP`

8. Sean has four computers in the test lab. He wants to install Windows Vista. The configurations for each of his computers are listed in the exhibit below. Place a mark on the computer that meets all of the minimum requirements for Windows Vista.




	Computer A	Computer B	Computer C	Computer D
Processor	Celeron 2.4GHz	PIII 600MHz	P4 1.6 GHz	Athlon XP 2000+
Memory	512MB	512MB	256MB	768MB
Free Disk Space	15GB	60GB	20GB	10GB

9. You are a consultant for a medium-sized business. Your client wants to upgrade his computers to Windows Vista, but is not sure which edition he should purchase. He wants his computers to support dual physical processors, Windows Aero, Remote Desktop, and integrated hardware-based drive encryption. Which Windows Vista edition should he purchase?

A. Windows Vista Home Premium

B. Windows Vista Business

C. Windows Vista Enterprise

D. Windows Vista Ultimate

10. Your computer is configured with two hard drives. You have decided to configure logical drive C: on disk 0 and logical drive D: on disk 1. You want to run Windows 98 for backward compatibility with some applications that will not run under Windows Vista. However, you also want to run Windows Vista to take advantage of the Windows Vista features. On drive D:, you want to store files that should have a high level of security. You will install Windows 98 on drive C: and Windows Vista on drive D:. How should the drives on this computer be configured?

A. Configure both logical drives as FAT32.

B. Configure both logical drives with NTFS.

C. Configure logical drive C: as FAT32 and logical drive D: as NTFS.

D. Configure logical drive C: as NTFS and logical drive D: as FAT32.

11. You are the network administrator of a large corporation. You manage a computer lab that is used for compatibility testing. Many of the computers are configured to support dual-booting of operating systems. One of the racks of computers is configured to dual-boot between Windows 98 and Windows Vista. Which of the following statements reflects proper configuration for these computers?

A. You should turn off disk compression on the Windows 98 configuration.

B. You should enable dynamic disks on the Windows Vista configuration.

C. You should install both operating systems into the same `Windows` directory so you can access applications under both operating systems.

D. You should edit the Registry on the Windows Vista computer for `HKEY_LOCAL_MACHINE\DualBoot` to a value of 1 so you can access applications under both operating systems.

12. You are the network administrator of a small company. You have decided to install Windows Vista on all of the company's computers. Because of your company's high security needs, your network is not connected to the Internet. After you installed Windows Vista, you did not perform the postinstallation activation because you did not have an Internet connection and have not had time to call the Microsoft Clearinghouse to properly complete postinstallation activation. After the grace period for postinstallation activation expires, which of the following actions will you not be able to perform until you activate the product?

    A. Reading files

    B. Writing files

    C. Logging on to the computer

    D. You are automatically required to activate the operating system before any further actions can be taken.

13. Timothy is the network administrator for a small company. While installing Windows Vista on a Windows XP computer, he finds that he is unable to select Upgrade from the list of installation options. What steps should Timothy perform to enable the Upgrade option?

    A. Boot using the Windows Vista DVD and allow the installation program to run.

    B. Boot using a floppy disk and run `setup.exe` from the Windows Vista DVD.

    C. Boot using a floppy disk and run `setup.exe` from a network share.

    D. Run `setup.exe` on the Windows Vista DVD from within the Windows XP operating system.

14. Eammon is the network administrator for a small company. He recently created a dual-boot configuration with Windows XP Professional and Windows Vista. Eammon needs the computer to boot to Windows XP Professional by default. What should Eammon use to modify the default operating system? (Choose all that apply.)

    A. `Boot.ini`

    B. `Bcdedit.exe`

    C. BIOS

    D. Select Control Panel ➢ Advanced System Settings ➢ Settings from the Windows Vista Control Panel

15. You are the network administrator for your company. You are attempting to install Windows Vista on a computer in the lab, but the installation process keeps failing halfway through. During the process of troubleshooting the Windows Vista installation, you decide to verify all of the actions that were taken during the Setup phase. Where can you find a log file that will tell you this information?

    A. `\Windows\verify.log`

    B. `\Logfiles\verify.log`

    C. `\Windows\setupact.log`

    D. `\Logfiles\setup.log`

16. Christine has a computer that is capable of booting to Windows 2000 Professional, Windows XP Home Edition, Windows Server 2003, and Windows Vista. Each operating system is contained on its own partition. After converting the Windows Vista partition to a dynamic disk, which of Christine's operating systems will not be able to see the Windows Vista partition?

A. Windows 2000 Professional

B. Windows XP Home Edition

C. Windows 2003 Server

D. None of these operating systems will be able to see the Windows Vista partition.

17. Robert is the IT director for a healthcare company. He wants to create a multiboot computer that can be used for testing clinical applications on a variety of operating systems, including DOS, Windows 98, Windows 2000 Professional, Windows XP Professional, and Windows Vista. In what way should he install the operating systems?

A. The operating systems should be installed from oldest to newest, and all operating systems should be placed in separate partitions.

B. The operating systems should be installed from oldest to newest, and all operating systems should be placed in the same partition.

C. The operating systems should be installed from newest to oldest, and all operating systems should be placed in separate partitions.

D. The operating systems should be installed from newest to oldest, and all operating systems should be placed in the same partition.

18. You are the network administrator for your company. You are installing Windows Vista on a computer that has many partitions already configured. When you reach the partition selection phase, you do not see an available partition that you want to use. Which of the following actions are you not able to perform after selecting Drive Options (advanced)?

A. Adding a partition

B. Contracting a partition

C. Deleting a partition

D. Extending a partition

19. Gary is a junior administrator at your company. He is attempting to configure his new Windows Vista computer to automatically download critical updates, service packs, and drivers, but he wants to be able to choose whether they are installed. He also wants to configure his computer to automatically download updates for Microsoft Office. How can Gary access these settings from the Control Panel? (Choose all that apply.)

A. From Windows Classic View, Gary can select Windows Update.

B. From Windows Category View, Gary can select Security Center ➢ Windows Update.

C. From Windows Classic View, Gary can select Automatic Updates.

D. From Windows Category View, Gary can select Security Center ➢ Automatic Updates.

20. Hayden is the network administrator of a toy distribution center in the United States. After receiving his Windows Vista DVD in the mail, he is surprised to discover that the DVD only contains four Windows Vista editions. Which Windows Vista editions are probably not included on his DVD? (Choose all that apply.)

A. Windows Vista Starter

B. Windows Vista Home Basic

C. Windows Vista Ultimate

D. Windows Vista Enterprise

Answers to Review Questions

1. B. The processor must be a Celeron or Pentium III 800MHz or better. A 1GHz processor is required to be considered a Windows Vista Premium Ready PC, but James is only required to have an 800MHz processor to install Windows Vista. You can verify the current requirements for Windows Vista at `http://www.microsoft.com/technet/windowsvista/evaluate/hardware/vistarpc.mspx`.

2. C. You must have a minimum of a 20GB drive with at least 15GB of free space to install Windows Vista. You can verify the current requirements for Windows Vista at `http://www.microsoft.com/technet/windowsvista/evaluate/hardware/vistarpc.mspx`.

3. A, D. The Windows Vista Upgrade Advisor is used to ensure that a computer's hardware components are supported by Windows Vista. The Hardware Compatibility List (HCL) can also be used to ensure compatibility with Windows Vista. The Hardware Compatibility List (HCL) shows the computers and components that have been tested to work with Windows Vista. When selecting hardware, you should always check for HCL compatibility. You can access the Windows Vista HCL at `https://winqual.microsoft.com/HCL/Default.aspx`.

4. C. If you have a disk device that does not have a driver on the Windows Vista DVD, and the manufacturer provides a Windows Vista driver, you can load the alternate driver by clicking Load Driver and browsing to the location where the driver is stored. You can load the driver from CD, DVD, or USB removable media.

5. A, C. Windows 2000 Professional and Windows XP Professional *x*64 cannot be upgraded to Windows Vista Business by performing an in-place upgrade; a clean install must be performed. The 32-bit version of Windows XP Professional and Windows XP Tablet PC can be upgraded to Windows Vista Business by performing an in-place upgrade.

6. C, D. Vince can perform an in-place upgrade to either Windows Vista Business or Windows Vista Ultimate. A clean install, which does not preserve applications or settings, would have to be performed in order to install Windows Vista Home Basic or Windows Vista Home Premium. Generally, if the Windows Vista installation would cause your existing installation to lose functionality, a clean install must occur.

7. B. Adam's files are stored in the `\Windows.old` directory. The files and folders that are moved to the `\Windows.old` directory include those contained within `Documents and Settings`, `Program Files`, and `Windows`.

8. A. You should have placed a mark on Computer A, which meets the minimum requirements of an 800MHz processor, 512MB of memory, and 15GB of free disk space. Computer B does not meet the minimum processor requirement. Computer C does not meet the minimum memory requirement. Computer D does not meet the free disk space requirement.

9. C. Your client should purchase Windows Vista Enterprise, which contains support for dual physical processors, Windows Aero, Remote Desktop, and BitLocker Drive Encryption. Windows Vista Business includes support for each of those features except the integrated hardware-based drive encryption offered by BitLocker. Windows Vista Home Premium lacks support for drive encryption, Remote Desktop, and dual physical processors. Windows Vista Ultimate contains each of the required features, but at a cost greater than that of Windows Vista Enterprise.

10. C. You should configure logical drive C: as FAT32 because Windows 98 will not read NTFS partitions. Logical drive D: should be configured as NTFS because you want to implement NTFS file system security. Windows Vista cannot be installed on a FAT partition.

11. A. You should turn off disk compression before you dual-boot. Windows Vista does not support the disk compression that was used by Windows 98. There is no way to configure the operating systems to recognize applications under both platforms. Windows Vista cannot be installed on a FAT partition, and Windows 98 cannot be installed on an NTFS partition. Windows 98 cannot read dynamic disks.

12. B. Once the grace period for product activation expires, you will not be able to write any changes to files or create new files until you activate the product.

13. D. To enable the Upgrade option, Timothy must run the `setup.exe` program from within Windows 2000, Windows XP, or Windows Vista. The `setup.exe` program can be run from the DVD or network share. It is not necessary to use a floppy disk to boot a computer before installing Windows Vista because the Windows Vista media is bootable.

14. B, D. Eammon should use the `Bcdedit.exe` utility or select Control Panel ➢ Advanced System Settings ➢ Settings from the Windows Vista Control Panel to modify the default operating system.

15. C. You can find the log file that details Setup actions in `\Windows\setupact.log`. This log can be useful in identifying installation errors.

16. B. Windows XP Home Edition will not be able to see the Windows Vista partition after it is converted to a dynamic disk. Windows NT 4.0 and Windows 9*x* operating systems are also not able to see Windows Vista dynamic disks.

17. A. Robert should install the operating systems from oldest to newest, and all operating systems should be placed in separate partitions. In fact, Windows Vista requires that it be installed in a separate partition in a dual- or multiple-boot configuration. Besides, if Robert is creating an environment for testing applications on each operating system, he will probably want the operating systems to be completely separate from one another.

18. B. You cannot contract a partition from the partition selection screen after selecting Drive Options (advanced). However, you are able to add, delete, extend, or format a partition.

19. A, B. From Windows Classic View, Gary can select Windows Update, or from Windows Category View, Gary can select Security Center ➢ Windows Update. The remaining two choices are used for configuring Automatic Updates on a Windows XP computer.

20. A, D. Windows Vista Starter and Windows Vista Enterprise are probably not included on this DVD. The standard Windows Vista DVD contains the Home Basic, Home Premium, Business, and Ultimate editions. The Windows Vista Starter edition is only available in developing countries; it is not available in the United States or the European Union. The Windows Vista Enterprise edition is only available through Microsoft Software Assurance or a Microsoft Enterprise Agreement.

Chapter

2

Automating the Windows Vista Installation

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Installing and Upgrading Windows Vista**

You can automate the installation of Windows Vista in several ways: by using an unattended installation, by using Windows Deployment Services (WDS) to remotely deploy unattended installations (which requires a Windows Server 2003 with SP1), or by using the System Preparation Tool for disk imaging. To help customize these options for automating remote installations, you can also use answer files. Answer files are used with automated installations to provide answers to the questions that are normally asked during the installation process. After you've installed Windows Vista, you can also automate the installation of applications by using Windows Installer packages.

This chapter begins with an overview of the automated deployment options available with Windows Vista. Then, this chapter describes how to access the deployment tools available for Windows Vista. Next, it details the use of unattended installation; WDS; how the System Preparation Tool, along with ImageX, is used to create disk images for automated installation; and how to use Windows System Image Manager (SIM) to create unattended answer files.

Choosing Automated Deployment Options

If you need to install Windows Vista on multiple computers, you could manually install the operating system on each computer, as described in Chapter 1, "Getting Started with Windows Vista." However, automating the deployment process will make your job easier, more efficient, and more cost effective if you have a large number of client computers to install. Windows Vista comes with several utilities that can be used for deploying and automating the Windows Vista installation. By offering multiple utilities with different functionality, administrators have increased flexibility in determining how to best deploy Windows Vista within a large corporate environment.

The following sections contain overviews of the automated deployment options, which will help you choose which solution is best for your requirements and environment. Each utility will then be covered in more detail throughout the chapter. The options for automated deployment of Windows Vista are

- Unattended installation, or unattended setup, which uses `Setup.exe`
- WDS, which requires Windows Server 2003 SP1 for deployment
- System Preparation Tool (`Sysprep.exe`), which is used to create and deploy disk imaging or cloning

Later in the chapter, you will see a table that summarizes the features and requirements of each installation deployment option.

You can also deploy Windows Vista through Systems Management Server (SMS), which is beyond the scope of this book. You can learn more about SMS on the Microsoft website at `http://www.microsoft.com`.

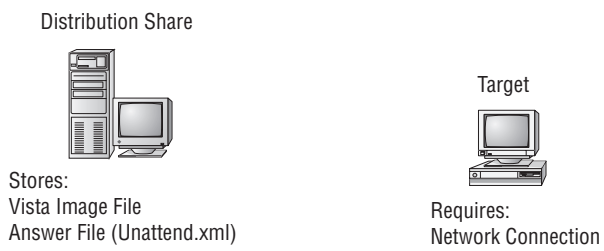
An Overview of Unattended Installation

Unattended installation is a practical method of automatic deployment when you have a large number of clients to install and the computers require different hardware and software configurations. Unattended installations utilize an answer file called `Unattend.xml` to provide configuration information during the unattended installation process. With an unattended installation, you can use a distribution share to install Windows Vista on the target computers. You can also use a Windows Vista DVD with an answer file located on the root of the DVD, on a floppy disk, or on a Universal Flash Device (UFD), such as an external USB flash drive.

Unattended installations allow you to create customized installations that are specific to your environment. Custom installations can support custom hardware and software installations. Since the answer file for Windows Vista is in XML format, all custom configuration information can be contained within the `Unattend.xml` file. This is different from past versions of Windows where creating automated installation routines for custom installations required multiple files to be used. In addition to providing standard Windows Vista configuration information, you can use the answer file to provide installation instructions for applications, additional language support, service packs, and device drivers.

If you use a distribution share, then the distribution share should contain the Windows Vista operating system image and the answer file to respond to installation configuration queries. The target computer must be able to connect to the distribution share over the network. After the distribution share and target computers are connected, you can initiate the installation process. Figure 2.1 illustrates the unattended installation process.

FIGURE 2.1 Unattended installation with distribution share and a target computer



Using and configuring unattended installations is covered in detail in the "Deploying Unattended Installations" section of this chapter.

Advantages of Unattended Installation

The advantages of using unattended installations as a method for automating Windows Vista installations include the following:

- Saves time and money because users do not have to interactively respond to each installation query.
- Can be configured to provide automated query response, while still selectively allowing users to provide specified input during installations.
- Can be used to install clean copies of Windows Vista or upgrade an existing operating system (providing it is on the list of permitted operating systems) to Windows Vista.
- Can be expanded to include installation instructions for applications, additional language support, service packs, and device drivers.
- The physical media for Windows Vista does not need to be distributed to all computers that will be installed.

Disadvantages of Unattended Installation

The disadvantages of using unattended installations as a method for automating Windows Vista installations include the following:

- Requires more initial setup than a standard installation of Windows Vista.
- Someone must have access to each client computer and must initiate the unattended installation process.

An Overview of Windows Deployment Services

Windows Deployment Services (WDS) is an updated version of Remote Installation Services (RIS). WDS is a suite of components that allows you to remotely install Windows Vista on client computers.

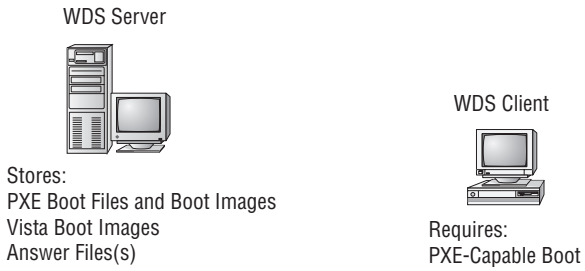
A WDS server installs Windows Vista on the client computers, as illustrated in Figure 2.2. The WDS server must be configured with the *Preboot Execution Environment* (PXE) boot files, the images to be deployed to the client computers, and the answer file. WDS client computers must be *PXE* capable. PXE is a technology that is used to boot to the network when no operating system or network configuration has been installed and configured on a client computer.

The WDS clients access WDS servers through the Dynamic Host Configuration Protocol (DHCP) to remotely install the operating system from the WDS server. The network environment

must be configured with a DHCP server, a Domain Name System (DNS) server, and Active Directory to connect to the WDS server. No other client software is required to connect to the WDS server. Remote installation is a good choice for automatic deployment when you need to deploy to large numbers of computers and the client computers are PXE compliant.

We discuss WDS installation in the "Using Windows Deployment Services (WDS)" section later in this chapter.

FIGURE 2.2 Windows Deployment Services (WDS) uses a WDS server and WDS clients.



Advantages of WDS

The advantages of using WDS as a method for automating Windows Vista installations include the following:

- Windows Vista installations can be standardized across a group or organization.
- The physical media for Windows Vista does not need to be distributed to all computers that will be installed.
- End-user installation deployment can be controlled through the Group Policy utility. For example, you can configure what choices a user can access or are automatically specified through the end-user Setup Wizard.

Disadvantages of WDS

The disadvantages of using WDS as a method for automating Windows Vista installations include the following:

- Can be used only if your network is running Windows Server 2003 with Active Directory installed.
- The clients that use WDS must be PXE capable.

An Overview of the System Preparation Tool and Disk Imaging

The System Preparation Tool (`Sysprep.exe`) is used to prepare a computer for disk imaging, which can then be captured using ImageX, a new imaging management tool included with Windows Vista. *Disk imaging* is the process of creating a *reference computer* for the automated deployment. The reference, or source, computer has Windows Vista installed and is configured with the settings and applications that should be installed on the target computers. An image is then created that can be transferred to other computers, thus installing the operating system, settings, and applications that were defined on the reference computer.

Using the System Preparation Tool and disk imaging is a good choice for automatic deployment when you have a large number of computers with similar configuration requirements. For example, education centers that reinstall the same software every week could use this technology to simplify their deployment process.

To perform an unattended install, the System Preparation Tool prepares the reference computer by stripping away any computer-specific data, such as the *security identifier (SID)*, which is used to uniquely identify each computer on the network, any event logs, and any other unique system information. The System Preparation Tool also detects any Plug and Play devices that are installed and can adjust dynamically for any computers that have different hardware installed.

When the client computer starts an installation using a disk image, you can customize what is displayed on the Windows Welcome screen and the options that are displayed through the setup process. You can also fully automate when and how the Windows Welcome screen is displayed during the installation process by using the `/oobe` option with the System Preparation Tool and an answer file named `Oobe.xml`.

The process for using the System Preparation Tool to create disk images is covered in detail in the "Using the System Preparation Tool to Prepare an Installation for Imaging" section later in this chapter.

Advantages of the System Preparation Tool

The advantages of using the System Preparation Tool as a method for automating Windows Vista installations include the following:

- For large numbers of computers with similar hardware, it greatly reduces deployment time by copying the operating system, applications, and Desktop settings from a reference computer to an image, which can then be deployed to multiple computers.
- Using disk imaging facilitates the standardization of Desktops, administrative policies, and restrictions throughout an organization.
- Reference images can be copied across a network connection or through DVDs that are physically distributed to client computers.

Disadvantages of the System Preparation Tool

The disadvantages of using the System Preparation Tool as a method for automating Windows Vista installations include the following:

- ImageX, third-party imaging software, or hardware disk-duplicator devices must be used for an image-based Setup.
- The version of the System Preparation Tool that shipped with Windows Vista must be used. An older version of `Sysprep` cannot be used on a Windows Vista image.
- Will not detect any hardware that is non–Plug and Play compliant.

Summary of Windows Vista Deployment Options

Table 2.1 summarizes the installation options for Windows Vista and notes the required client hardware, server requirements, and whether the option supports a clean install or upgrade.

TABLE 2.1 Summary of Windows Vista Installation Options

	Attended Installation	Unattended Installation	WDS	System Preparation Tool
Required Client Hardware	PC that meets Windows Vista requirements	PC that meets Windows Vista requirements, access to the network	PC that meets the Windows Vista requirements that is PXE compliant	Reference computer with Windows Vista installed and configured; PC that meets the Windows Vista requirements; ImageX, third-party disk imaging software, or hardware disk-duplicator device
Required Server Hardware and Services	None	None with DVD; if using network installation, distribution server with preconfigured client images	Windows Server 2003 w/ SP1 to act as a WDS server with image files, Active Directory, DNS server, and DHCP server	None
Clean Install or Upgrade Only	Clean install or upgrade	Clean install or upgrade	Clean install	Clean install

Table 2.2 summarizes the unattended installation tools and files that are used with automated installations of Windows Vista, the associated installation method, and a description of each tool.

TABLE 2.2 Summary of Windows Vista Unattended Deployment Utilities

Tool or File	Automated Installation Option	Description
`Setup.exe`	Unattended installation	Program used to initiate the installation process
`Unattend.xml`	Unattended installation	Answer file used to customize installation queries
`Windows System Image Manager`	Unattended installation	Program used to create answer files to be used for unattended installations
`ImageX.exe`	Sysprep	Command-line utility that works in conjunction with Sysprep to create and manage Windows Vista image files for deployment
`Sysprep.exe`	Sysprep	System Preparation Tool, which prepares a source reference computer that will be used in conjunction with a distribution share or with disk duplication through ImageX, third-party software, or hardware disk-duplication devices

Accessing the Windows Vista Deployment Tools

The Windows Vista installation utilities and resources relating to automated deployment are found in a variety of locations. Table 2.3 provides a quick reference for each utility or resource and its location.

TABLE 2.3 Location of Windows Vista Deployment Utilities and Resources

Utility	Location
`Sysprep.exe`	Included with Windows Vista; installed to `%WINDIR%\system32\sysprep`

TABLE 2.3 Location of Windows Vista Deployment Utilities and Resources *(continued)*

Utility	Location
ImageX	Installed with the Windows Automated Installation Kit (WAIK); installed to `C:\Program Files\Windows AIK\Tools\x86\imagex.exe`
Windows System Image Manager	Installed with WAIK; installed to `C:\Program Files\Windows AIK\Tools\Image Manager\ImgMgr.exe`

The Windows Automated Installation Kit (WAIK) is available in the Business Desktop Deployment 2007 Toolkit available for download from `http://connect.microsoft.com`.

Deploying Unattended Installations

You can deploy Windows Vista installations or upgrades through a Windows Vista distribution DVD or through a distribution server that contains Windows Vista images and associated files, such as `Unattend.xml` for unattended installations. Using a DVD can be advantageous if the computer on which you want to install Windows Vista is not connected to the network or is connected via a low-bandwidth network. It is also typically faster to install a Windows Vista image from DVD than to use a network connection.

Unattended installations rely on options configured in an answer file that is deployed with the Windows Vista image. Answer files are XML files that contain the settings that are typically supplied by the installer during attended installations of Windows Vista. Answer files can also contain instructions for how programs and applications should be run.

You will learn more about answer files in the section "Using Windows System Image Manager to Create Answer Files" later in this chapter.

The Windows Setup program is run to install or upgrade to Windows Vista from computers that are running compatible versions of Windows, as discussed in Chapter 1. In fact, Windows Setup is the basis for the other types of installation procedures we'll be discussing in this chapter, including unattended installations, WDS, and image-based installations.

The Windows Setup program (`Setup.exe`) replaces `Winnt32.exe` and `Winnt.exe`, which are the setup programs used in previous versions of Windows. Although a graphical tool, Windows Setup can be run from the command line. For example, you can use the following command to initiate an unattended installation of Windows Vista:

```
setup.exe /unattend:answerfile
```

The Windows Setup program has several command-line options that can be applied. Table 2.4 describes the `Setup.exe` command-line options.

TABLE 2.4 Setup.exe Command-Line Options and Descriptions

Setup.exe Option	Description
`/1394debug:` *channel* `[baudrate:`*baudrate*`]`	Enables kernel debugging over a FireWire (IEEE 1394) port for troubleshooting purposes. The `[baudrate]` optional parameter specifies the baud rate for data transfer during the debugging process.
`/debug:`*port* *[baudrate:baudrate]*	Enables kernel debugging over the specified port for trouble-shooting purposes. The `[baudrate]` optional parameter specifies the baud rate for data transfer during the debugging process.
`/dudisable`	Used to prevent a dynamic update from running during the installation process.
`/emsport:{com1|com2|usebiossettings|off}` `[/emsbaudrate:`*baudrate*`]`	Configures EMS to be enabled or disabled. The `[baudrate]`optional parameter specifies the baud rate for data transfer during the debugging process.
`/m:`*folder_name*	Used with Setup to specify that replacement files should be copied from the specified location. If the files are not present, then Setup will use the default location.
`/noreboot`	Normally, when the downlevel phase of `Setup.exe` is complete, the computer restarts. This option specifies that the computer should not restart so that you can execute another command prior to the restart.
`/tempdrive:`*drive letter*	Specifies the location that will be used to store the temporary files for Windows Vista and the installation partition for Windows Vista.
`/unattend:`*[answerfile]*	Specifies that you will be using an unattended installation for Windows Vista. The `answerfile` variable points to the custom answer file you will use for installation.

Using Windows Deployment Services (WDS)

You can remotely install Windows Vista by using WDS. WDS is included with WAIK. For WDS installation, you need a WDS server that stores the Windows Vista operating system

files in a shared image folder, and clients that can access the WDS server. Depending on the type of image you will distribute, you may also want to configure answer files so that users need not respond to any Windows Vista installation prompts. (Answer files are described in the "Using Windows System Image Manager to Create Answer Files" section of this chapter.)

The following are some of the advantages of using WDS for automated installation:

- You can remotely install Windows Vista.
- The procedure simplifies management of the server image by allowing you to access Windows Vista distribution files from a distribution server.
- You can quickly recover the operating system in the event of a computer failure.

Here are the basic steps of the WDS process from a PXE-enabled WDS client:

1. The WDS client initiates a special boot process through the PXE network adapter (and the computer's BIOS configured for a network boot). On a PXE client, the client presses F12 to start the PXE boot process and to indicate that they want to perform a WDS installation.
2. A list of available Windows Preinstallation Environment (PE) boot images is displayed. The client should select the appropriate Windows PE boot image from the boot menu.
3. The Windows Welcome screen is displayed. The client should click the Next button.
4. The WDS client is prompted to enter credentials for accessing and installing images from the WDS server.
5. A list of available operating system images is displayed. The client should select the appropriate image file to install.
6. The WDS client is prompted to enter the product key for the selected image.
7. The Partition and Configure the Disk screen is displayed. This screen provides the ability to install a mass storage device driver, if needed, by pressing F6.
8. The image copy process is initiated, and the selected image is copied to the WDS client computer.

The following sections describe how to set up the WDS server and the WDS clients and how to install Windows Vista through WDS.

Preparing the WDS Server

With the WDS server, you can manage and distribute Windows Vista operating system images to WDS client computers. The WDS server contains any files necessary for PXE booting, Windows PE boot images, and the Windows Vista images to be deployed.

The following steps for preparing the WDS server are discussed in the upcoming sections:

1. Make sure the server meets the requirements for running WDS.
2. Install WDS.
3. Configure and start WDS.
4. Configure the WDS server to respond to client computers (if this was not configured when WDS was installed).

Meeting the WDS Server Requirements

For WDS to work, the server on which you will install WDS must meet the requirements for WDS and be able to access the required network services.

WDS Server Requirements

The WDS server must meet these requirements:

- The computer must be a domain controller or a member of an Active Directory domain.
- The WAIK must be installed.
- At least one partition on the server must be formatted as NTFS.
- Remote Installation Services (RIS) must be installed. WDS is an updated version of RIS and requires RIS to be installed, although RIS does not need to be configured on the server.
- A network adapter installed.

Network Services

The following network services must be running on the WDS server or be accessible to the WDS server from another network server:

- TCP/IP, installed and configured.
- A DHCP server, which is used to assign DHCP addresses to WDS clients. (Ensure that your DHCP scope has enough addresses to accommodate all the WDS clients that will need IP addresses.)
- A DNS server, which is used to locate the Active Directory controller.
- Active Directory, which is used to locate WDS servers and WDS clients, as well as to authorize WDS clients and manage WDS configuration settings and client installation options.

Installing the WDS Server Components

To configure WDS, you should first install the WAIK. Then, you can install the WDS Update package from WDS directory located within the directory where WAIK was installed. As part of the WDS installation, the following are loaded on the server (these are required for the WDS server to function properly):

TFTP The *Trivial File Transfer Protocol (TFTP)* is a User Datagram Protocol (UDP)–based file transfer protocol that is used to download the Windows PE from the WDS server to the WDS clients.

WDS Service The WDS service provides the services needed to manage the WDS process.

WDS MMC snap-in The WDS MMC snap-in and other WDS management utilities are installed, which provide graphical interfaces for managing WDS on the server.

Configuring WDS on the Server

You can configure WDS on a Windows Server 2003 computer by using the Windows Deployment Services Configuration Wizard or by using the WDSUTIL command-line utility. To configure WDS on the server, you will need to perform the following actions:

- Create a shared folder that will be used to store the Windows Vista images, the Windows PE boot images, and any files necessary for booting using PXE.
- Create the Windows PE and Windows Vista images.
- Configure the PXE listener to determine how the server will handle WDS client requests.

The WDS Setup Wizard provides a graphical interface that can be used to configure WDS on the server. To configure WDS using the WDS Setup Wizard, you should do the following:

1. Click Start ➢ Administrative Tools ➢ Windows Deployment Services.
2. Right-click Windows Deployment Services node, and click Add Server.
3. Select the Local Computer (the computer this console is running on) option.
4. Expand the Servers node.
5. Right-click the newly added server, and click Configure Server.
6. Configure the remote installation folder location, or accept the default location, which is `C:\RemoteInstall`.
7. Configure the PXE listener options on the PXE Server Initial Settings page. For example, if you want the WDS server to respond to any WDS client computer contacting it, then you should select the Respond to All Client Computers option. You can also configure the WDS client to be automatically added to the server by clicking Advanced and clicking Auto-Add the Client Computer and Mark It As Known.
8. Clicking Finish will end the WDS configuration process on the server.

The WDSUTIL command-line utility can be used to perform the same configuration options from a command prompt. Table 2.5 describes the WDSUTIL command-line options.

TABLE 2.5 WDSUTIL Command-Line Options and Descriptions

WDSUTIL Option	Description
`/initialize`	Initializes the configuration of the WDS server
`/uninitialize`	Undoes any changes made during the initialization of the WDS server
`/add`	Adds images and devices to the WDS server
`/convert`	Converts Remote Installation Preparation (RIPrep) images to WIM images
`/remove`	Removes images from the server

TABLE 2.5 WDSUTIL Command-Line Options and Descriptions *(continued)*

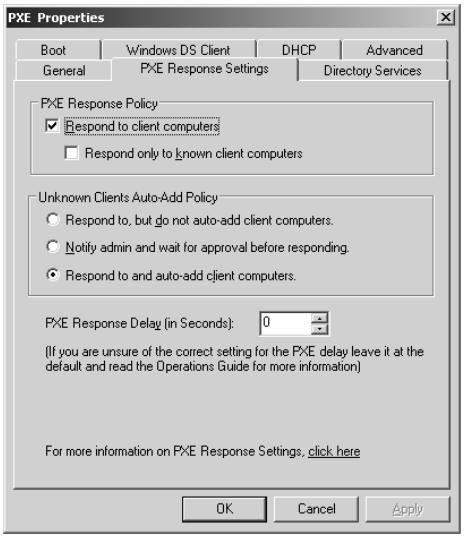
WDSUTIL Option	Description
`/set`	Sets information in images, image groups, WDS servers, and WDS devices
`/get`	Gets information from images, image groups, WDS servers, and WDS devices
`/new`	Creates new capture images or discover images
`/copy`	Copies images from the image store
`/export`	Exports to WIM files images contained within the image store
`/start`	Starts WDS services
`/stop`	Stops WDS services
`/disable`	Disables WDS services
`/enable`	Enables WDS services
`/approve`	Approves Auto-Add devices
`/reject`	Rejects Auto-Add devices
`/delete`	Deletes records from the Auto-Add database
`/update`	Uses a known good resource to update a server resource

Configuring the WDS Server to Respond to Client Requests

The WDS server must be configured to respond to client requests. You can configure the server response as a part of the WDS server installation or do it later, after the WDS server is installed and ready for client requests. Take the following steps to configure the WDS server on a Windows Server 2003 computer to respond to client requests:

1. Select Start ➢ Administrative Tools ➢ Windows Deployment Services.
2. The Windows Deployment Services window appears. Expand the Servers node, right-click your server, then select PXE Server Settings.
3. In the PXE Properties dialog box, select the Respond to Client Computers check box, then select the Respond to and Auto-Add Client Computers check box, as shown in Figure 2.3.
4. Close the Windows Deployment Services window.

FIGURE 2.3 The PXE Properties dialog box of the WDS snap-in



Preparing the WDS Client

The WDS client is the computer on which Windows Vista will be installed. WDS clients rely on a technology called PXE, which allows the client computer to remotely boot and connect to a WDS server.

To act as a WDS client, the computer must meet all the hardware requirements for Windows Vista (see Chapter 1) and have a PXE-capable network adapter installed, and a WDS server must be present on the network. Additionally, the user account used to install the image must be a member of the Domain Users group in Active Directory.

Installing Windows Vista through WDS

After the WDS server has been installed and configured, you can install Windows Vista on a WDS client that uses a PXE-compliant network card.

To install Windows Vista on the WDS client, follow these steps:

1. Start the computer. When prompted, press F12 for a network service boot.
2. The Windows PE is displayed.
3. The Windows Welcome screen is displayed. Click the Next button to start the installation process.
4. Enter the username and password of an account that has permissions to access and install images from the WDS server.

5. A list of available operating system images stored on the WDS server will be displayed. Select the image to install, and click Next.
6. Enter the product key for the selected Windows Vista image, and click Next.
7. The Partition and Configure the Disk screen is displayed. Select the desired disk partitioning options, or click OK to use the default options.
8. Click Next to initiate the image copying process. The Windows Setup process will begin after the image is copied to the WDS client computer.

Using the System Preparation Tool to Prepare an Installation for Imaging

You can use disk images to install Windows Vista on computers that have similar hardware configurations. Also, if a computer is having technical difficulties, you can use a disk image to quickly restore it to a baseline configuration.

To create a disk image, you install Windows Vista on the source computer with the configuration that you want to copy and use the System Preparation Tool to prepare the installation for imaging. The source computer's configuration should also include any applications that should be installed on target computers.

Once you have prepared the installation for imaging, you can use imaging software such as ImageX to create an image of the installation.

The System Preparation Tool (`Sysprep.exe`) is included with Windows Vista, in the `%WINDIR%\system32\sysprep` directory. When you run this utility on the source computer, it strips out information from the master copy that must be unique for each computer, such as the SID.

Table 2.6 defines the command options that you can use to customize the `Sysprep.exe` operation.

TABLE 2.6 System Preparation Command-Line Options

Switch	Description
`/audit`	Configures the computer to restart into audit mode, which allows you to add drivers and applications to Windows or test the installation prior to deployment
`/generalize`	Removes any unique system information from the image, including the SID and log information
`/oobe`	Specifies that the Windows Welcome screen should be displayed when the computer reboots

TABLE 2.6 System Preparation Command-Line Options *(continued)*

Switch	Description
`/quiet`	Runs the installation with no user interaction
`/quit`	Specifies that the System Preparation tool should quit after the specified operations have been completed
`/reboot`	Restarts the target computer after the System Preparation Tool completes
`/shutdown`	Specifies that the computer should shut down after the specified operations have been completed
`/unattend`	Indicates the name and location of the answer file to use

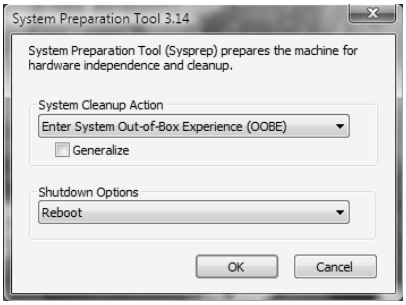
In the following sections, you will learn how to create a disk image and how to copy and install from a disk image.

Preparing a Windows Vista Installation

To run the System Preparation Tool and prepare an installation for imaging, take the following steps:

1. Install Windows Vista on a source computer. The computer should have a similar hardware configuration to the destination computer(s). The source computer should not be a member of a domain. (See Chapter 1 for instructions on installing Windows Vista.)
2. Log on to the source computer as an Administrator and, if desired, install and configure any applications, files (such as newer versions of Plug and Play drivers), or custom settings (for example, a custom Desktop) that will be applied to the target computer(s).
3. Verify that your image meets the specified configuration criteria and that all applications are properly installed and working.
4. Select Start ➢ Computer, and navigate to `C:\%WINDIR%\System32\sysprep`. Double-click the Sysprep application icon.
5. The Windows System Preparation Tool dialog box appears, as shown in Figure 2.4. Select the appropriate options for your configuration.
6. If configured to do so, Windows Vista will be rebooted into setup mode, and you will be prompted to enter in the appropriate setup information.
7. You will now be able to use imaging software to create an image of the computer to deploy to other computers.

FIGURE 2.4 The Windows System Preparation Tool dialog box



In Exercise 2.1, you will use the System Preparation Tool to prepare the computer for disk imaging.

EXERCISE 2.1

Using the System Preparation Tool

1. Log on to the source computer as Administrator and, if desired, install and configure any applications that should also be installed on the target computer.
2. Select Start ➢ Computer, and navigate to `C:\%WINDIR%\System32\sysprep`. Double-click the Sysprep application icon.
3. In the System Preparation Tool dialog box, select the options to use to configure the image, and then click the OK button.
4. Depending on the options selected, the System Preparation Tool will quit, the computer will shut down, or the computer will be rebooted into setup mode, where you will need to configure the setup options.

Using ImageX to Create a Disk Image

After you've run the System Preparation Tool on the source computer, you can create an image from the installation, and you can then install the image on target computers.

To create an image, you can use ImageX, which is a command-line utility that can be used to create and manage Windows Image (`.wim`) files.

Creating a Disk Image

To run the ImageX utility to create a disk image of a Windows Vista installation, follow these steps:

1. Reboot the computer into the Windows PE.

2. At the resulting command prompt, access by the ImageX utility by typing **D:\Tools\ImageX** and entering the appropriate options. For example, to create an image named Windows Vista, you could enter the following command:

```
D:\ImageX.exe /capture C: C:\Images\image.wim "Windows Vista" /verify
```

3. You can copy the new image to a network share or to the local computer for hardware disk duplication. To copy the image to a network share, you can use the `net use [dir] [network share]` command along with the `copy [file] [dir]` command to copy the file.

In Exercise 2.2, you will use the ImageX utility to create a disk image of a Windows Vista installation.

EXERCISE 2.2

Using the ImageX Utility to Create a Disk Image

1. Boot the computer into the Window PE.
2. Type the following command in Windows PE, assuming that your DVD\CD drive is configured as drive D:

```
D:\ImageX.exe /capture C: C:\Images\image.wim "Windows Vista" /verify
```

3. Copy the new image to a network share at `\\Server\Images` by using the following commands:

```
net use z: \\Server\Images

copy  C:\Images\image.wim z:
```

Installing from a Disk Image

After you've run the System Preparation Tool and ImageX on the source computer, you can copy the image and then install it on the target computer.

After the image is copied, you should boot the destination computer into the Windows PE. If the computer has been used previously, it may be necessary to reformat the hard drive, which you can do using the `diskpart` command in Windows PE. If the image is stored over the network, you should then copy the image to the destination computer by using the `net use [dir] [network share]` and `copy [file] [dir]` commands. Then, you should use the `/apply` option of the ImageX utility to apply the image to the local computer. If an answer file has not been deployed along with the image, you may have to apply such information as regional settings, the product key, computer name, and password to the new computer after the destination computer is rebooted.

If you have created an answer file for use with disk images, as described in the upcoming section "Using Windows System Image Manager to Create Answer Files," the installation will run without requiring any user input.

In Exercise 2.3, you will use the stripped image that was created in Exercise 2.2 to simulate the process of continuing an installation from a disk image.

EXERCISE 2.3

Installing Windows Vista from a Disk Image

1. Boot the target computer into the Windows PE environment.
2. Copy the image created in Exercise 2.2 to the local computer by using the following commands:

```
net use z: \\Server\Images

copy  Z:\Images\image.wim C:
```

3. Apply the image to the target computer using the following ImageX command:

```
D:\ImageX.exe /apply C:\Images\image.wim C:
```

Using Windows System Image Manager to Create Answer Files

Answer files are automated installation scripts used to answer the questions that appear during a normal Windows Vista installation. You can use answer files with Windows Vista unattended installations, disk image installations, or WDS installations. Setting up answer files allows you to easily deploy Windows Vista to computers that may not be configured in the same manner, with little or no user intervention. Because answer files are associated with image files, you can validate the settings within an answer file against the image file.

You can create answer files by using the *Windows System Image Manager (SIM)* utility. There are several advantages to using Windows SIM to create answer files:

- You can easily create and edit answer files through a graphical interface, which reduces syntax errors.
- It simplifies the addition of user-specific or computer-specific configuration information.
- You can validate existing answer files against newly created images.
- You can include additional application and device drives to the answer file.

In the following sections, you will learn about options that can be configured through Windows SIM, how to create answer files with Windows SIM, how to format the answer file, and how to manually edit answer files.

Configuring Components through Windows System Image Manager

You can use Windows SIM to configure a wide variety of installation options. The following list defines what components can be configured through Windows SIM and gives a short description of each component:

auditSystem Adds additional device drivers, specifies firewall settings, and applies a name to the system when the image is booted into audit mode. Audit mode is initiated by using the `sysprep /audit` command.

auditUser Executes `RunSynchronous` or `RunAsynchronous` commands when the image is booted into audit mode. Audit mode is initiated by using the `sysprep /audit` command.

generalize Removes system-specific information from an image so that the image can be used as a reference image. The settings specified in the generalize component will only be applied if the `sysprep /generalize` command is used.

offlineServicing Specifies the language packs and packages to apply to an image prior to the image being extracted to the hard disk.

oobeSystem Specifies the settings to apply to the computer the first time that the computer is booted into the Windows Welcome screen, which is also known as the Out-Of-Box Experience (OOBE). To boot to the Welcome Screen, the `sysprep /oobe` command should be used.

specialize Configures the specific settings for the target computer, such as network settings and domain information. This configuration pass is used in conjunction with the generalize configuration pass.

Windows PE Sets the Windows PE–specific configuration settings, as well as several Windows Setup settings, such as partitioning and formatting the hard disk, selecting an image, and applying a product key.

Creating Answer Files with Windows System Image Manager

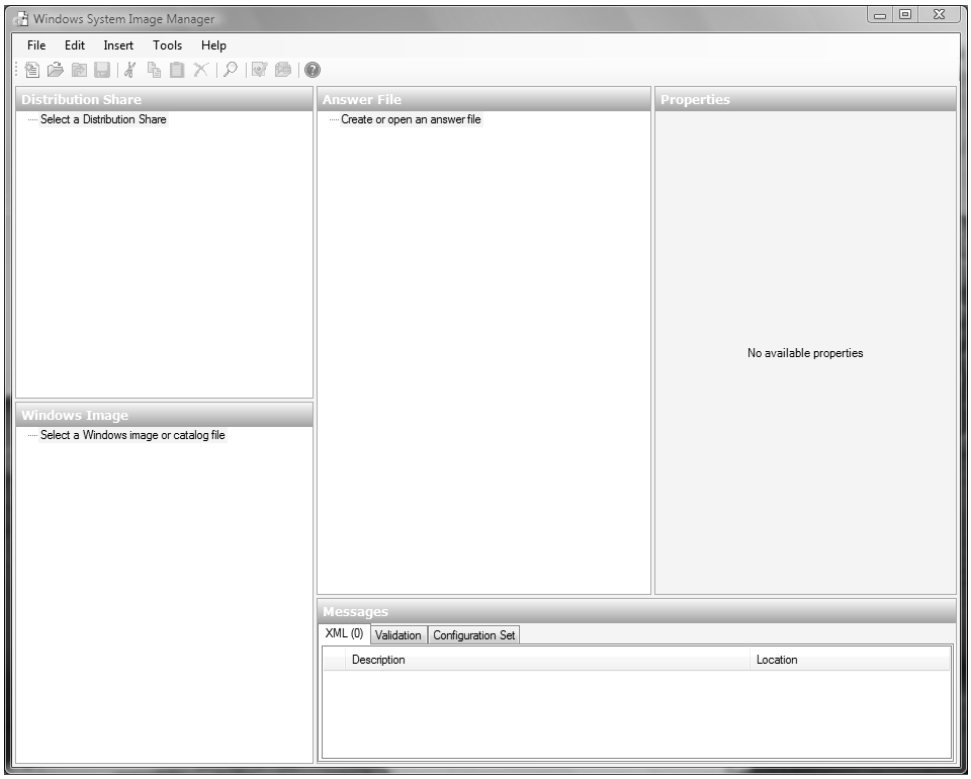
After you have installed the WAIK, you can run the Windows SIM utility to create a new answer file or edit existing answer files.

The following steps describe how to create a new answer file using Windows SIM:

1. Select Start ➢ All Programs ➢ Microsoft Windows AIK, and click Windows System Image Manager.

2. Windows System Image Manager displays an empty screen with five panes: a pane for selecting distribution shares, a pane for selecting Windows image files, the answer file pane, a properties pane, and a pane for displaying validation messages, as shown in Figure 2.5.
3. Select the Windows Vista image file for which a new answer file should be created by clicking the File ➢ Select Windows Image option or by right-clicking the Windows Image pane in Windows SIM and clicking Select Windows Image.
4. Select File ➢ New Answer File or right-click the Answer File pane and select New Answer File from the context menu to generate the structure of the new answer file.
5. Right-click each component as desired to modify the configuration pass options that are specific to the new environment. You can drill down within a component to provide specific customizations, or you can modify parent-level components.
6. When you have finished customizing the answer file for the desired environment, click File ➢ Save Answer File to save the answer file.

FIGURE 2.5 Windows System Image Manager Startup Screen



You can use an answer file to provide automated answers for a DVD-based installation. Simply create a new answer file named `Unattend.xml` and copy it to the root of the DVD. Insert the Windows Vista DVD and set the BIOS to boot from the DVD drive. As the installation begins, Windows Setup will implicitly search for answer files in a number of locations, including the root of removable media drives.

Summary

In this chapter, you learned how to install Windows Vista through automated installation. We covered the following topics:

- An overview of the three common methods for automated installation: unattended installations, Windows Deployment Services (WDS), and using the System Preparation Tool along with ImageX
- How to use WDS, including installing and configuring the WDS server as well as the requirements for the WDS clients
- Preparing an installation for imaging by using the System Preparation Tool (`Sysprep.exe`)
- Creating a disk image by using the ImageX utility
- Using unattended answer files to automatically respond to the queries that are generated during a normal installation process

Exam Essentials

Know the difference between unattended installation methods. Understand the various options available for unattended installations of Windows Vista and when it is appropriate to use each installation method.

Understand how to use unattended installation for Windows Vista deployment. Know when it is appropriate to use unattended installations for Windows Vista deployment.

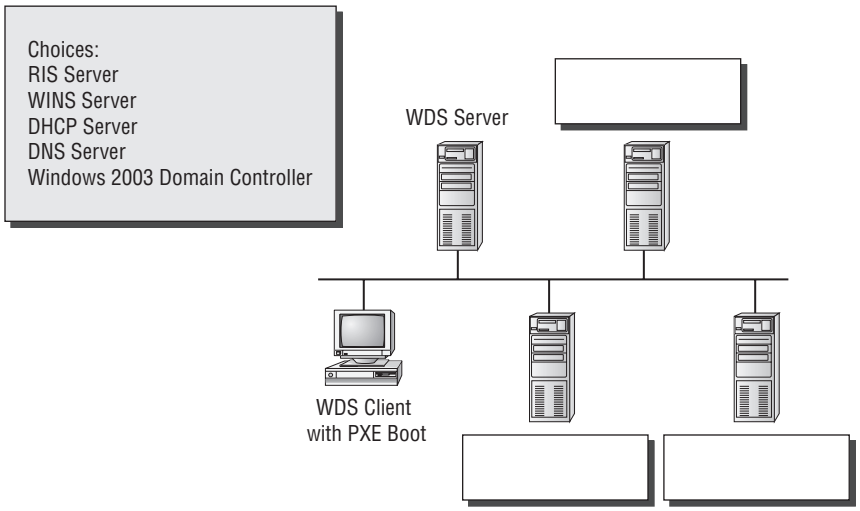
Understand the features and uses of WDS. Know when it is appropriate to use WDS to manage unattended installations. Be able to list the requirements for setting up WDS servers and WDS clients. Be able to complete an unattended installation using WDS.

Be able to use disk images for unattended installations. Know how to perform unattended installations of Windows Vista using the System Preparation Tool and disk images.

Know how to use Windows System Image Manager to create and edit answer files. Understand how to access and use Windows System Image Manager to create answer files. Be able to edit the answer files and know the basic options that can be configured for answer files.

Review Questions

1. You are the network administrator of a large corporation. Your company has decided to use WDS to install 100 client computers. You have set up the WDS server and now want to test a single WDS client to make sure that the installation will go smoothly. In the following diagram, select and place the servers that need to be on the network to support the WDS installation:



2. You are the network administrator for Widgets R Us. You are in charge of developing a plan to install 200 Windows Vista computers in your company's data center. You decide to use WDS. You are using a Windows Server 2003 domain and have verified that your network meets the requirements for using WDS services. What command-line utility should you use to configure the WDS server?

   A. ImageX

   B. WDSUTIL

   C. `Setup.exe`

   D. The WDS icon in Control Panel

3. Your company has a variety of client computers that are running Windows 2000 Professional. You want to upgrade these machines to Windows Vista using WDS. What requirement must be met on a client computer to upgrade to Windows Vista from a WDS server?

   A. The computer must use a PXE-based boot ROM.

   B. The computer must contain an NTFS partition.

   C. The computer must use identical hardware configurations as the reference image.

   D. There is no option to upgrade with WDS.

4. Curtis is the network manager for a large company. He has been tasked with creating a deployment plan to automate installations for 100 computers that need to have Windows Vista installed. Curtis wants to use WDS for the installations. To fully automate the installations, he needs to create an answer file. He does not want to create the answer files with a text editor. What other program can he use to create unattended answer files via a GUI interface?
   A. ImageX
   B. Answer Manager
   C. Windows System Image Manager
   D. System Preparation Tool

5. Bob is using WDS to install 100 clients that are identically configured. The first 65 computers are installed with no problems. When he tries to install the other 35, he receives an error and the installation process will not begin. Which of the following would cause this failure?
   A. The WDS server has been authorized to serve only 65 clients.
   B. The WINS server is no longer available.
   C. The DHCP server does not have enough IP addresses to allocate to the WDS clients.
   D. The network bandwidth has become saturated.

6. You run a training department that needs the same software installed from scratch on the training computers each week. You decide to use ImageX to deploy disk images. Which Windows Vista utility can you use in conjunction with ImageX to create these disk images?
   A. UAF
   B. Answer Manager
   C. Setup Manager
   D. System Preparation Tool

7. You are trying to decide whether you want to use WDS as a method of installing Windows Vista within your company. Which of the following options is NOT an advantage of using a WDS automated installation?
   A. The Windows Vista security is retained when you restart the computer.
   B. Windows Vista installation media does not need to be deployed to each computer.
   C. Unique information is stripped out of the installation image so that it can be copied to other computers.
   D. You can quickly recover the operating system in the event of a system failure.

8. You are the network manager of the XYZ Corporation. You are in charge of developing an automated deployment strategy for rolling out new Windows Vista computers. You want to install a WDS server and are evaluating whether an existing server can be used as a WDS server for Windows Vista deployment. Which of the following is NOT a requirement for configuring the WDS server?
   A. The remote installation folder must be NTFS version 3.0 or later.
   B. The remote installation folder must reside on the system partition.
   C. RIS must be installed on the server.
   D. The existing server must run Windows Server 2003 with Service Pack 1 installed.

9. You are using WDS to install 20 Windows Vista computers. When the clients attempt to use WDS, they are not able to complete the unattended installation. You suspect that the WDS server has not been configured to respond to client requests. Which one of the following utilities would you use to configure the WDS server to respond to client requests?

A. Active Directory Users and Computers

B. Active Directory Users and Groups

C. WDS MMC snap-in

D. WDSMAN

10. You want to install a group of 25 computers using disk images created in conjunction with the System Preparation Tool. Your plan is to create an image from a reference computer and then copy the image to all the machines. You do not want to create a SID on the destination computer when you use the image. Which `Sysprep.exe` command-line option should you use to set this up?

A. `/specialize`

B. `/generalize`

C. `/oobe`

D. `/quiet`

11. You are planning on deploying 100 new computers throughout your company. Each new computer is similarly configured. You want to create a reference image that will then be applied to the remaining images. Which of the following utilities should you use?

A. WDSUTIL

B. `Setup.exe`

C. Windows SIM

D. ImageX

12. You are a network technician for your company, and you need to deploy Windows Vista to multiple computers. You want to automate the installation of Windows Vista so that no user interaction is required during the installation process. Which of the following utilities could you use?

A. Windows SIM

B. ImageX

C. `System Preparation Tool`

D. WDSUTIL

13. You want to initiate a new installation of Windows Vista from the command line. You plan to accomplish this by using the `Setup.exe` command-line setup utility. You want to use an answer file with this command. Which command-line option should you use?

A. `/unattend`

B. `/apply`

C. `/noreboot`

D. `/generialize`

14. You have manually created an answer file that you want to use to deploy an image that you have previously created. Before deploying the image, you want to ensure that your answer file will work with the image. Which of the following tools could you use to validate the answer file?
    A. System Preparation Tool
    B. Windows SIM
    C. ImageX
    D. WDSUTIL

15. You have created a Windows Vista image that you will copy to a DVD and deploy to several new computers. You want to use an answer file to automate the setup process. Where should the answer file be located so that you can use it during installation?
    A. On a network share
    B. On a WDS server
    C. On a separate DVD
    D. At the root of the DVD

16. You are planning on deploying a new Windows Vista image to 100 client computers that are similarly configured. You are using the Windows SIM tool to create an answer file that will be used to automate the installation process. You want each computer to contain two partitions, one for the system partition and one that will function as a data partition. You need to modify the answer file to support this configuration. Which component of the answer file will you need to modify?
    A. oobeSystem
    B. auditSystem
    C. windowsPE
    D. specialize

17. Your company has recently hired a new employee. You need to deploy Windows Vista on the new employee's computer. You have previously created a Windows Vista image using the ImageX utility that you have successfully deployed to other computers. You want to use ImageX to deploy the image to the new employee's computer. Which ImageX option will you need to use?
    A. `/apply`
    B. `/capture`
    C. `/mount`
    D. `/verify`

18. You are using WDS to deploy Windows Vista images across your organization, and you are using the WDSUTIL command-line utility to perform this task. You want to copy a previously created image from the image store using this utility. Which option of WDSUTIL should you use?
    A. `/move`
    B. `/copy`
    C. `/get`
    D. `/enable`

19. You are using the Windows SIM tool to create an answer file to be used when deploying new Windows Vista images. You are editing the configuration passes to so that the desired settings are entered during the installation process. You are currently editing the specialize component of the answer file. Which of the following information should you include in this component of the answer file?

A. Hard disk partitioning information

B. Product key information

C. `Windows Welcome screen settings`

D. Domain and network settings

20. You have recently installed Windows Vista onto a reference computer that will be used to create an image that can then be deployed to sales employees' computers. You have installed and configured several proprietary sales applications on the computer. You have previously used the System Preparation Tool to remove any system-specific information from the computer, and you plan to use ImageX to create the image from this reference computer. Which option of the ImageX utility can you use to accomplish your goal?

A. `/apply`

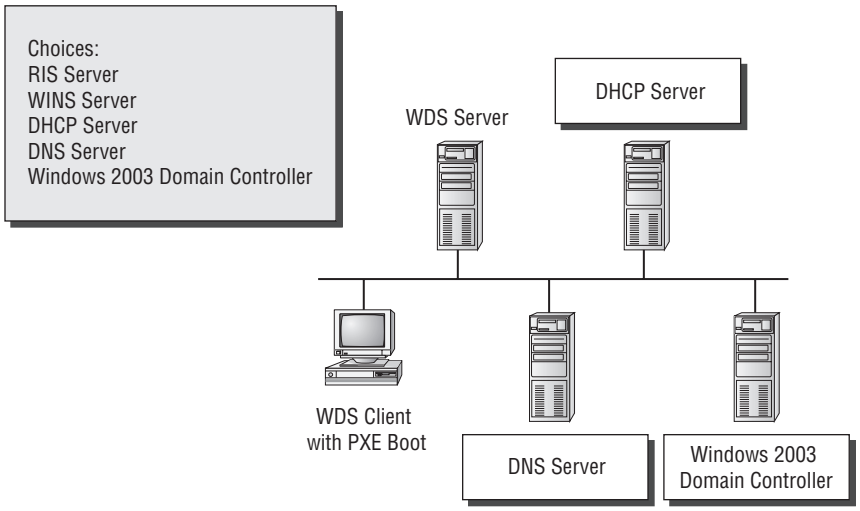
B. `/capture`

C. `/mount`

D. `/verify`

Answers to Review Questions

1. Here is the answer:



   DNS, DHCP, and the Active Directory must be properly configured and running for WDS services to work. The WDS server must also be installed and configured.

2. B. WDSUTIL is a command-line utility that can be used to configure the WDS server. Several other configuration options need to be specified on the WDS server that you can set using WDSUTIL.

3. D. If you are using WDS, it is not possible to upgrade from Windows 2000 Professional; you can only install a fresh copy of Windows Vista. Unattended installations can be used to support automated upgrades.

4. C. Windows System Image Manager (SIM) is used to create unattended answer files in Windows Vista. It uses a GUI-based interface to set up and configure the most common options that are used within an answer file.

5. C. To access the WDS server, the WDS clients must be able to access the DHCP server. Each WDS client will use an IP address from the DHCP server's scope, so you should ensure that the DHCP server has enough addresses to accommodate all of the WDS clients.

6. D. Once you have a reference computer installed, you can use the System Preparation Tool to prepare the computer to be used with disk imaging. ImageX is a utility that can be used to create a disk image after it is prepared using the System Preparation Tool. The image can then be transferred to the destination computer(s).

7. C. Unique information is stripped out of the installation image when you use the System Preparation Tool to create a disk image—for example, the unique SID that is applied to every computer. Unique information is then generated when the target computer is installed.

8. B. When you configure your WDS server, the remote installation folder should not reside on the system partition.

9. C. You enable WDS servers to respond to client requests through the Windows Deployment Services (WDS) Microsoft Management Console (MMC) snap-in. In the PXE Properties dialog box, enable the option Respond to Client Computers.

10. B. The `/generalize` options prevents system-specific information to be included in the image. The `Sysprep.exe` command can be used with a variety of options. You can see a complete list by typing **sysprep /?** at a command-line prompt.

11. D. ImageX is a command-line utility that can be used to create and manage Windows Vista image (WIM) files. You can configure a reference installation that is configured as desired, and then use ImageX to create an image of the installation that can then be deployed to the remaining computers.

12. A. SIM is a graphical utility that can be used to create an answer file. Answer files can be used to automate the installation routine so that no user interaction is required.

13. A. The `/unattend` option can be used with the `Setup.exe` command to initiate an unattended installation of Windows Vista. You should also specify the location of the answer file to use when using the `Setup.exe` utility.

14. B. You can use the SIM tool to validate an answer file, even if the answer file was manually created in a text editor.

15. D. During a DVD-based setup, an answer file can be used to automate the installation process. The Windows Setup program implicitly searches for an answer file in several locations, including the root of the DVD.

16. C. You would configure formatting and partitioning information in the windowsPE component of the answer file. The options specified in this configuration pass will occur before the image will be copied to the local computer.

17. A. To deploy the Windows Vista image using ImageX, you will need to use the `/apply` option. This option applies the selected image to a specified drive volume.

18. B. You should use the `/copy` option of the WDSUTIL utility to copy an image from the image store.

19. D. The specialize component of the answer file will contain information specific to the target computer, such as domain information and network settings.

20. B. To create a Windows Vista image from a reference computer using the ImageX utility, you should use the `/capture` option. This option captures the image into a new WIM file.

Chapter 3

Configuring the Windows Vista Environment

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring and Troubleshooting Post-Installation System Settings**
  - Troubleshoot post-installation configuration issues
  - Configure and troubleshoot Windows Aero
- ✓ **Maintaining and Optimizing Systems that Run Windows Vista**
  - Troubleshoot reliability issues by using built-in diagnostic tools
- ✓ **Configuring and Troubleshooting Mobile Computing**
  - Configure mobile display settings
  - Configure mobile devices
  - Configure Tablet PC software
  - Configure power options

After you've installed Windows Vista, you will need to install and configure your hardware. The easiest hardware devices to install are those that follow the Plug and Play standard. However, it's not that difficult to install legacy, non–Plug and Play hardware by using the Device Manager Microsoft Management Console snap-in.

In this chapter, you will examine the process of configuring the Windows Vista environment, beginning with an overview of the main configuration utilities. Then you will learn how to update drivers. Next, you will see how to configure many different types of hardware, including disk devices, display devices, mobile computer hardware, I/O devices, and imaging devices. Finally, you will learn how to configure and manage Windows Vista services and multiple hardware profiles.

Using the Windows Vista Management Utilities

Windows Vista includes several utilities for managing various aspects of the operating system configuration. In the following sections, you will learn about the Microsoft Management Console, the Registry Editor, and Device Manager.

Using the Microsoft Management Console

The *Microsoft Management Console (MMC)* is the console framework for management applications. The MMC provides a common environment for *snap-ins*, which are administrative tools developed by Microsoft or third-party vendors. The MMC offers many benefits, including the following:

- The MMC is highly customizable—you add only the snap-ins you need.
- Snap-ins use a standard, intuitive interface, so they are easier to use than previous versions of administrative utilities.
- You can save and share MMC consoles with other administrators.

- You can configure permissions so that the MMC runs in authoring mode, which an administrator can manage, or in user mode, which limits what users can access.
- You can use most snap-ins for remote computer management.

As shown in Figure 3.1, by default the MMC console contains three panes: a console tree on the left, a details pane in the middle, and an optional Actions pane on the right. The console tree lists the hierarchical structure of all snap-ins that have been loaded into the console. The details pane contains a list of properties or other items that are part of the snap-in that is highlighted in the console tree. The Actions pane provides a list of actions that the user can access depending on the item selected in the details pane.

On a Windows Vista computer, there is no item created for the MMC by default. To open the console, click the Start button and type **MMC** in the Search dialog box. When you first open the MMC, it contains only the `Console Root` folder, as shown in Figure 3.2. The MMC does not have any default administrative functionality. It is simply a framework used to organize administrative tools through the addition of snap-in utilities.

FIGURE 3.1 The MMC console tree, details pane, and Actions pane

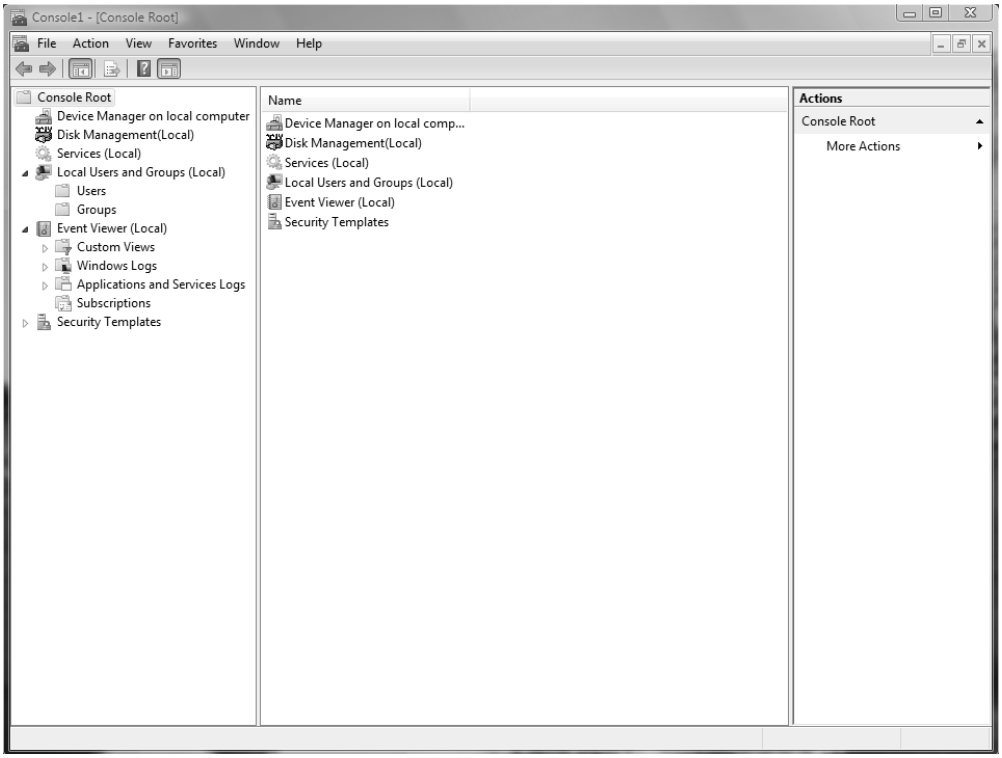
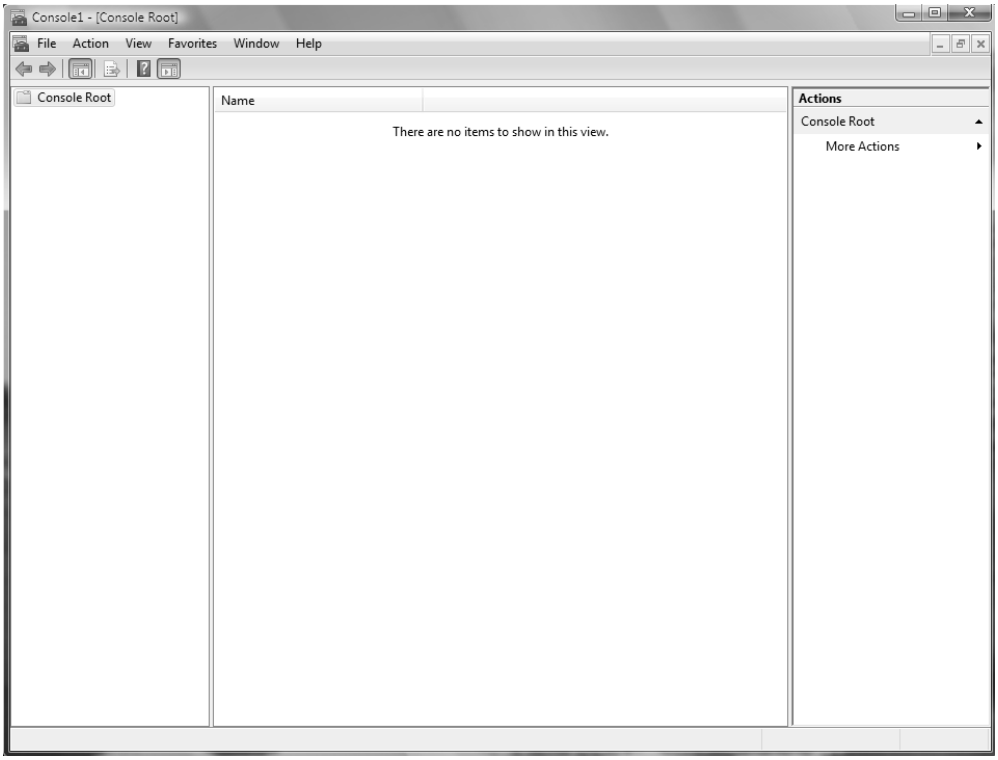


FIGURE 3.2 The opening MMC window



Configuring MMC Modes

You can configure the MMC to run in author mode, for full access to the MMC functions, or in one of three user modes, which have more limited access to the MMC functions. To set a console mode, select File ➢ Options to open the Options dialog box. In this dialog box, you can select from the console modes listed in Table 3.1.

TABLE 3.1 MMC Console Modes

Console Mode	Description
Author mode	Allows use of all the MMC functions.
User mode—full access	Allows users full access to window management commands, but they cannot add or remove snap-ins or change console properties.

TABLE 3.1 MMC Console Modes *(continued)*

Console Mode	Description
User mode—limited access, multiple window	Allows users to create new windows, but not close any existing windows. Users can access only the areas of the console tree that were visible when the console was last saved.
User mode—limited access, single window	Allows users to access only the areas of the console tree that were visible when the console was last saved, and they cannot create new windows.

Adding Snap-Ins

To add snap-ins to the MMC console and save it, take the following steps:

1. From the main console window, select File ➢ Add/Remove Snap-In to open the Add/Remove Snap-In dialog box.
2. Highlight the snap-in you want to add, and click the Add button.
3. If prompted, specify whether the snap-in will be used to manage the local computer or a remote computer. Then click the Finish button.
4. Repeat steps 2 and 3 to add each snap-in you want to include in your console.
5. When you have finished adding snap-ins, click OK.
6. Click OK to return to the main console screen.
7. After you have added snap-ins to create a console, you can save it by selecting File ➢ Save As and entering a name for your console. You can save the console to a variety of locations, including a program group or the Desktop. By default, custom consoles have an `.msc` extension.

In exercises in later chapters, you will add MMC snap-ins to create different custom consoles and save them in various locations. This will give you an idea of the flexibility of the MMC and how you can set up custom consoles for your administrative tasks.

Using the Registry Editor

The *Registry* is a database used by the operating system to store configuration information. You use the *Registry Editor* program to edit the Registry. This utility is designed for advanced configuration of the system. Usually, when you make changes to your configuration, you use other utilities, such as Control Panel.

Only experienced administrators should use the Registry Editor. It is intended for making configuration changes that can be made only directly through the Registry. For example, you might edit the Registry to specify an alternate location for a print spool folder. Improper changes to the Registry can cause the computer to fail to boot. Use the Registry Editor with extreme caution.

Windows Vista uses the REGEDIT program as the primary utility for Registry editing in Windows Vista. It supports full editing of the Registry. To use REGEDIT, select Start and type **REGEDIT** in the Search dialog box.

The REGEDIT program that is included with Windows Vista includes full search capabilities and full Registry support. You can still use REGEDT32 from the Search dialog box, but it will redirect you to the REGEDIT utility.

The Registry is organized in a hierarchical tree format of keys and subkeys that represent logical areas of computer configuration. By default, when you open the Registry Editor, you see five Registry key listings, as shown in Figure 3.3 and described in Table 3.2.

FIGURE 3.3 The Registry Editor window

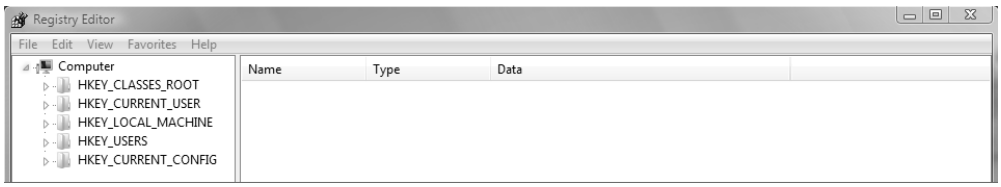


TABLE 3.2 Registry Keys

Registry Key	Description
HKEY_CURRENT_USER	Configuration information for the user who is currently logged on to the computer. This key is a subkey of the HKEY_USERS key.
HKEY_USERS	Configuration information for all users of the computer.
HKEY_LOCAL_MACHINE	Computer hardware configuration information. This computer configuration is used regardless of the user who is logged in.

TABLE 3.2 Registry Keys *(continued)*

Registry Key	Description
HKEY_CLASSES_ROOT	Configuration information used by Windows Explorer to properly associate file types with applications.
HKEY_CURRENT_CONFIG	Configuration of the hardware profile that is used during system startup.

Using Device Manager

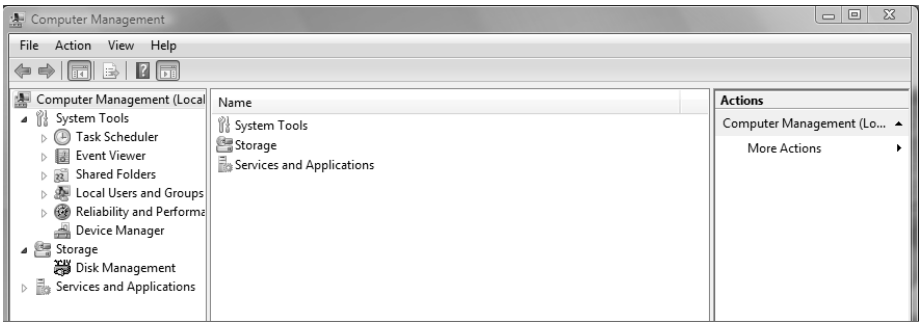
Device Manager displays information about the hardware that is installed on your computer and how it is configured. You can use Device Manager to ensure that all devices are working properly, configure your devices, and troubleshoot device problems. The specific actions you can take through Device Manager include the following:

- Viewing a list of all hardware that is installed on your computer
- Determining which device driver is installed for each device
- Updating device drivers
- Changing hardware settings
- Disabling, enabling, and uninstalling devices
- Using driver rollback to roll back to a previous version of a driver
- Troubleshooting device problems
- Printing a summary of all devices that are installed on your computer

Follow these steps to access Device Manager:

1. Select Start, right-click Computer, and select Manage from the context menu.
2. The Computer Management dialog box will open, as shown in Figure 3.4.

FIGURE 3.4 The Computer Management dialog box



3. Select Device Manager to see a list of all of the components that are installed on your computer, as shown in Figure 3.5.
4. Expand any device category by clicking the plus sign to see a list of all devices within that category, as shown in Figure 3.6.

If Device Manager detects that there is a problem with a specific device, the following icons will indicate what type of problem you have:

- A blue *i* on a white field indicates that the User Automatic Settings feature is not selected for the devices and that the resource has been manually selected. If you see this icon, no problem may be indicated and the device is not disabled.
- A black down arrow is used to specify that the device is disabled. This means that Windows Vista can recognize the device, but no protected mode driver is installed and enabled for the device.
- A black exclamation point (!) on a yellow field specifies that there is some problem with the device. The device may or may not be running.

We cover how to use Device Manager throughout this chapter.

FIGURE 3.5 Device Manager

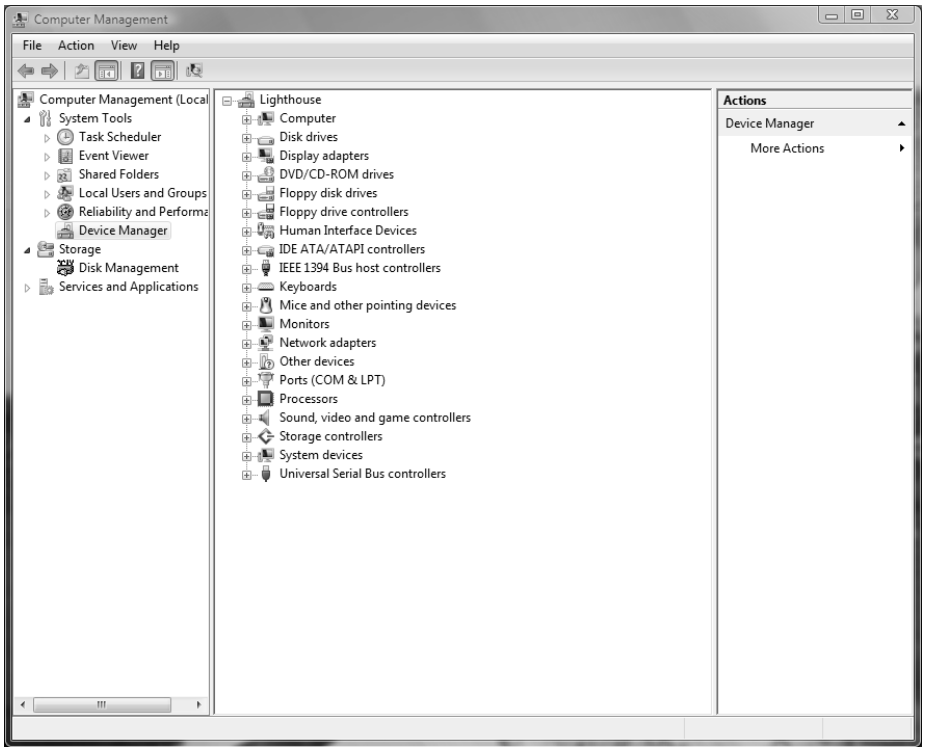
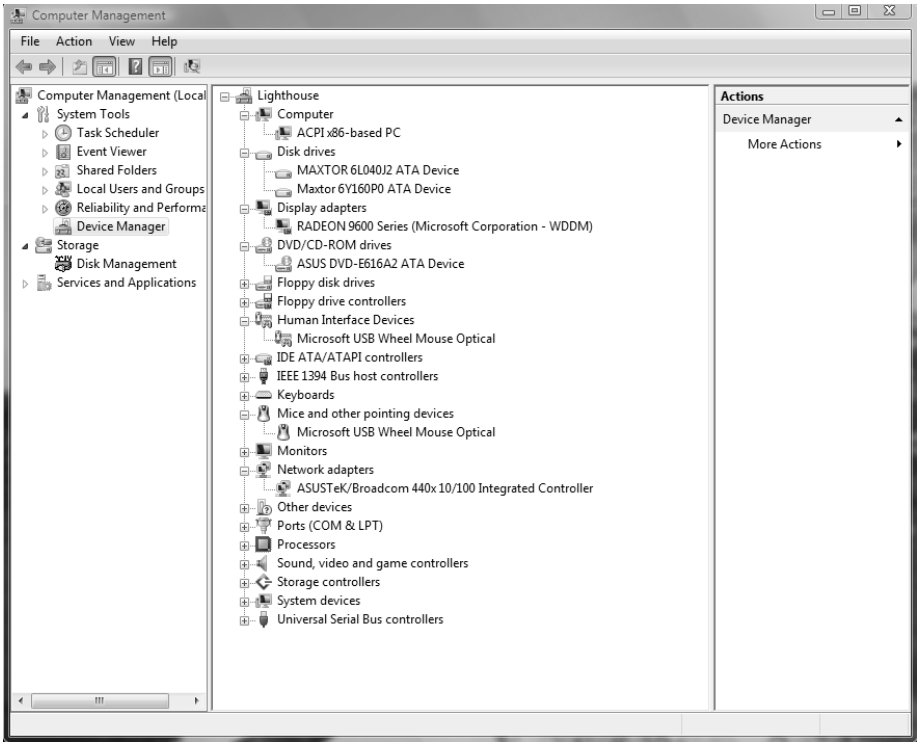


FIGURE 3.6 Device Manager, expanded window



Installing Hardware

If you buy new hardware, it will most likely be Plug and Play capable. If you need to use legacy, non–Plug and Play hardware, it is likely that you will have to configure the hardware to be properly recognized by the operating system.

Installing Plug and Play Devices

Plug and Play technology uses a combination of hardware and software that allows the operating system to automatically recognize and configure new hardware without any user intervention. Windows Vista Plug and Play support includes the following features:

- Automatic and dynamic recognition of hardware that is installed
- Automatic resource allocation (or reallocation, if necessary)

- Determination of the correct driver that needs to be loaded for hardware support
- Support for interaction with the Plug and Play system
- Support for power management features

Installing Non–Plug and Play Devices

Legacy or non–Plug and Play–capable hardware is also supported by Windows Vista. When you install legacy hardware, you need to configure it just as you did before Plug and Play technology was introduced.

First, you need to configure the hardware device's resources manually on the device or through a software configuration program. Hardware resources include the device's interrupt request (IRQ), I/O port address, memory address, and Direct Memory Access (DMA) settings. Before you configure the resources for the new device, determine which resources are available. You can view a listing of the currently allocated resources in the Device Manager utility, as follows:

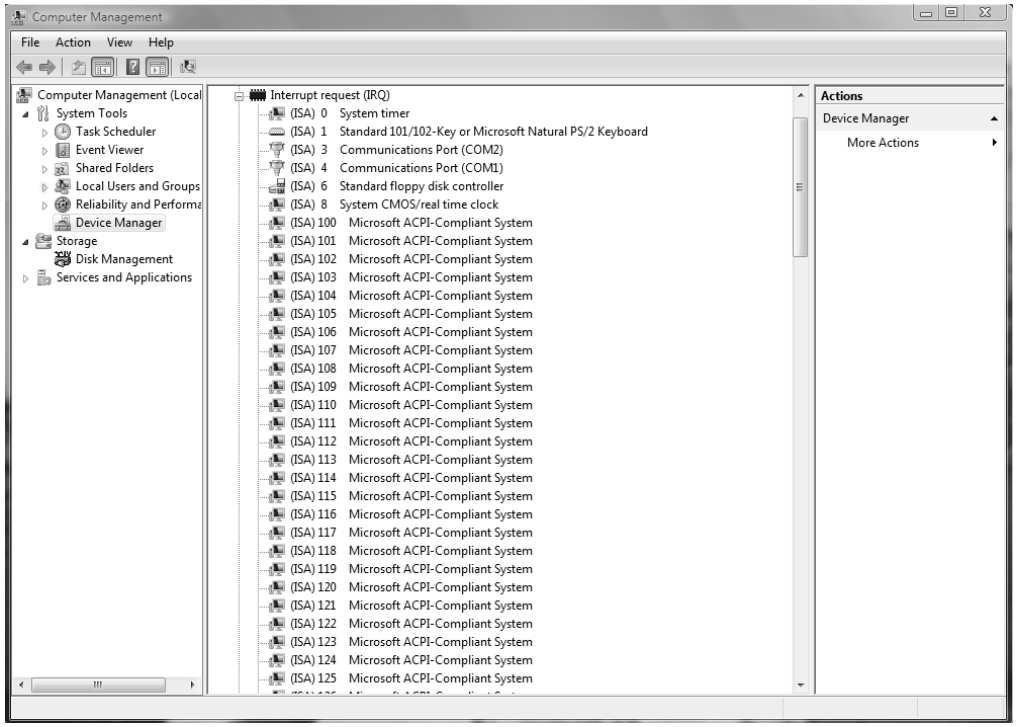
1. From the Start menu, right-click Computer and select Manage. In the Computer Management window, select System Tools and then Device Manager.
2. Select View ➢ Resources by Connection.
3. Device Manager displays a list of the current resources. Double-click a resource and then click the Resources tab to see all of the allocated resources of that type. Figure 3.7 shows an example of an IRQ listing in Device Manager.

Through View ➢ Resources by Type, you can see a listing for Direct Memory Access (DMA), Input/Output (IO), Interrupt Request (IRQ), and Memory. By expanding each resource type, you will see all devices that have been assigned resources within the category. This view is useful when you are determining which resources are in use and which resources are available.

After you've configured the hardware resources, you can use the Add Hardware icon in Control Panel (Classic View) to add the new device to Windows Vista and install the device driver. If the device is not listed, you will need a manufacturer-provided driver. Insert the disk that contains the driver and click the Have Disk button in Add Hardware.

You can also access Device Manager by right-clicking Computer in the Start menu and then selecting Properties, then selecting Device Manager. Windows Vista often offers several alternatives for completing the same task. Throughout this book, you will be presented with some of the different options for completing the same tasks.

FIGURE 3.7 Viewing resource allocation in Device Manager



Managing and Updating Device Drivers

A *device driver* is software that allows a specific piece of hardware to communicate with the Windows Vista operating system. Many devices have drivers that are included on the Windows Vista distribution media. Managing device drivers involves updating them when necessary and deciding how to handle drivers that may not have been properly tested.

Device manufacturers periodically update device drivers to add functionality or enhance driver performance. The updated drivers are typically posted on the manufacturer's website.

Exercise 3.1 takes you through the steps to update a device driver. To complete this exercise, you need to have an updated driver for one of your hardware devices.

EXERCISE 3.1

Updating a Device Driver

1. Select Start, right-click Computer, and select Manage from the context menu.
2. The Computer Management window opens. Select System Tools, then Device Manager.
3. The details pane lists all the devices that are installed on your computer. Right-click the device whose driver you want to update.
4. Select Update Driver Software from the context menu. The Update Driver Software dialog box will be displayed.
5. Select the Browse My Computer for Driver Software option.
6. In the Browse for Driver Software on Your Computer window, you can select a folder in which the driver is located, or you can select the Let Me Pick from a List of Device Drivers on My Computer option to pick the driver from a list. This exercise assumes that you will be installing your new driver from installation media provided by the device manufacturer. In this case, click the Browse button to browse to the installation media, and click Next.
7. The files will be installed for your driver. A window will be displayed indicating that Windows has successfully updated your driver software. Click the Close button to close this dialog box.
8. You may see a dialog box indicating that you must restart your computer before the change can be successfully implemented. If necessary, restart your computer.

Windows Vista provides an option called Roll Back Driver. You can use this option to roll back to a previously installed driver in the event that the new driver is installed and is faulty. To roll back a driver, select Roll Back Driver on the Driver tab through the device's properties in Device Manager.

Managing Disk Devices

You can manage disk devices through the Device Manager utility. The following sections describe how to manage CD-ROM, DVD, and removable media devices. We cover how to manage disks in Chapter 7, "Configuring Disks."

You install DVDs and CD-ROMs as you would any Plug and Play or non–Plug and Play device. We discussed how to install Plug and Play and non–Plug and Play devices previously in this chapter in the "Installing Hardware" section.

Managing DVD and CD-ROM Devices

DVDs and CD-ROMs are listed together under DVD/CD-ROM drives in Device Manager. Double-click DVD/CD-ROM Drives, and then double-click the device you want to manage. This opens the device Properties dialog box, which has five tabs:

General Lists the device type, manufacturer, and location. It also shows the device status, which indicates whether the device is working properly. If the device is not working properly, you can click the Troubleshoot button at the lower right of the dialog box to get some help with resolving the problem.

DVD Region Plays regionally encoded DVDs for a maximum of five regional changes.

Volumes Is used to display CD properties such as disk, type, status, partition style, capacity, unallocated space, and reserved space.

Driver Shows information about the currently loaded driver, as well as buttons that allow you to see driver details, uninstall the driver, roll back the driver, or update the driver. (See the "Managing and Updating Device Drivers" section earlier in the chapter for details on updating a driver.)

Details Displays a list of properties for the device and their values.

Right-clicking DVD/CD-ROM Drives in Device Manager gives you the option of updating the driver, disabling the device, uninstalling the device, scanning for hardware changes, or viewing the properties of the device.

In Exercise 3.2, you will manage disk devices.

EXERCISE 3.2

Managing Disk Devices

1. Select Start, and then right-click Computer and select Manage. In Computer Management, select System Tools and then Device Manager.
2. Double-click DVD/CD-ROM Drives, and then double-click the DVD or CD-ROM device you want to manage.

EXERCISE 3.2 *(continued)*

3. In the General tab of the device Properties dialog box, verify that your device is working properly. If the device is not working properly, click the Troubleshoot button. The Troubleshooter Wizard will ask you a series of questions and attempt to help you resolve the problem.
4. Click the Driver tab. Note the information about the currently loaded driver. This tab will allow you to update the driver, disable the device, or uninstall the driver.
5. Click OK to save your settings and close the dialog box.

Managing Removable Media

Removable media are devices such as tape devices and external hard drives. Like with DVD and CD-ROM devices, you can manage removable media through Device Manager.

Removable media are listed under Disk Drives in Device Manager. Double-click Disk Drives, and then double-click the removable media device you want to manage. This opens the device Properties dialog box. The General and Driver tabs are similar to those for CD-ROM and DVD devices, as described in the preceding section.

Managing Display Devices

A *video adapter* is the device that outputs the display to your monitor. You install a video adapter in the same way that you install other hardware. If it is a Plug and Play device, all you need to do is shut down your computer, add the video adapter, and turn on your computer. Windows Vista will automatically recognize the new device.

You can configure several options for your video adapters, and if you have multiple monitors with their own video adapters, you can configure multiple-display support. The following sections describe video adapter configuration and how to configure your computer to support multiple monitors.

You install video adapters as you would any Plug and Play or non–Plug and Play device. We discussed how to install Plug and Play and non–Plug and Play devices earlier in the chapter in the "Installing Hardware" section.

Configuring Video Adapters

The options for video settings are on the Monitor tab of the Display Settings dialog box, as shown in Figure 3.8. To access this dialog box, select Control Panel ➢ Appearance and

Personalization ➢ Personalization ➢ Display Settings. Alternatively, you could right-click an empty area on your Desktop, select Personalize from the pop-up menu, and then select Display Settings.

The Colors option in the Monitor tab sets the color quality, for example, to 32-bit quality or 16-bit quality, for your video adapter. The Resolution option allows you to set the screen resolution for your video adapter.

Other options are available for customizing the appearance of your Desktop. We discuss these options in Chapter 4, "Configuring the Windows Vista Desktop."

To configure advanced settings for your video adapter, click the Advanced button in the lower-right corner of the Monitor tab. This opens the Properties dialog box for the monitor, as shown in Figure 3.9.

You'll see four tabs with options for your video adapter and monitor.

Adapter Allows you to view and configure the properties of your video adapter.

Monitor Allows you to view and configure the properties of your monitor, including the refresh frequency (how often the screen is redrawn).

A lower refresh frequency setting can cause your screen to flicker. Setting the refresh frequency too high can damage some hardware.

FIGURE 3.8 The Monitor tab of the Display Settings dialog box

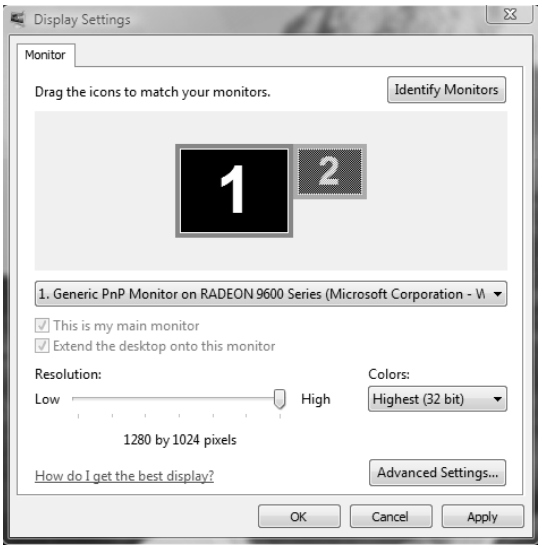
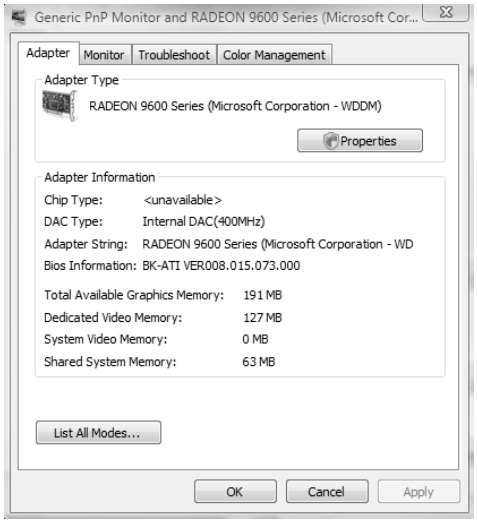


FIGURE 3.9 The Properties dialog box for a display monitor



Troubleshoot Allows you to configure how Windows Vista uses your graphics hardware. For example, you can configure hardware acceleration settings.

Color Management Allows you to select color profiles (the colors that are displayed on your monitor).

In Exercise 3.3, you will view the properties of your video adapter.

Usually, the video adapter is configured for typical use. Be careful if you change these settings because improper settings may cause your display to be unreadable.

EXERCISE 3.3

Viewing Video Adapter Settings

1. Right-click an empty area on the Desktop, choose Personalize, and select Display Settings.
2. Click the Advanced Settings button at the bottom of the Monitor tab. Make a note of your current settings in the Adapter tab.
3. Click the Monitor tab. Make a note of your current settings.

EXERCISE 3.3 *(continued)*

4. Click the Troubleshoot tab. Make a note of your current settings.
5. Click OK to close the monitor Properties dialog box.
6. Click OK to close the Display Settings dialog box.

Setting the Video's Resolution, Color Selection, and Refresh Rate

Depending on your video adapter, you can configure a monitor's resolution, color selection, and refresh rate. *Resolution* specifies how densely packed the pixels are. The more pixels, or dots per inch (dpi), the clearer the image. The SVGA (Super Video Graphics Adapter) standard is 1024×768, but many current models can display higher resolution, for example, 1600×1200. The color selection specifies how many colors are supported by your video adapter; for example, the monitor may be displaying 16 colors or 256 colors. *Refresh rate* indicates how many times per second the screen is refreshed (redrawn). To avoid flickering, this rate should be set to at least 72Hz.

Certain applications require specific configurations based on the graphics used. If you run across an application that requires a specific resolution, color selection, or refresh rate, or if a user makes a request based on personal preferences, you can easily determine what options are supported by the video adapter. In Control Panel, select Appearance and Personalization ➢ Personalization ➢ Display Settings ➢ Advanced Settings ➢ Adapter ➢ List All Modes.

Using Multiple-Display Support

Windows Vista allows you to extend your Desktop across multiple monitors. This means you can spread your applications across multiple monitors.

Setting Up Multiple-Display Support

To set up multiple-display support, you must have a video adapter installed that supports multiple monitors or a separate video adapter installed for each monitor.

If your computer has the video adapter built into the system board, you should install Windows Vista before you install the second video adapter. This is because Windows Vista will disable the video adapter that is built into the system board if it detects a second video adapter. When you add a second video adapter after Windows Vista is installed, it will automatically become the primary video adapter.

In Exercise 3.4, you will configure multiple-display support.

EXERCISE 3.4

Configuring Multiple-Display Support

1. Turn off your computer and install the new video adapters, if needed. Plug your monitors into the video adapters and turn on your computer. Assuming that the adapters are Plug and Play–compatible, Windows Vista will automatically recognize your new adapters and load the correct drivers.
2. Open the Display Settings dialog box (right-click an empty area on your Desktop, select Personalize, and click Display Settings). You should see an icon for each of the monitors.
3. Click the number of the monitor that will act as your additional display. Then select the Extend the Desktop Onto This Monitor check box. Repeat this step for each additional monitor you want to configure.

   You can arrange the order in which the displays are arranged by dragging and dropping the monitor icons in the Monitor tab of the Display Settings dialog box.
4. When you have finished configuring the monitors, click OK to close the dialog box.

Troubleshooting Multiple-Display Support

If you are having problems with multiple-display support, use the following troubleshooting guidelines:

The Extend the Desktop Onto This Monitor option isn't available. If the Monitor tab of the Display Settings dialog box doesn't give you the option Extend the Desktop Onto This Monitor, confirm that your secondary adapter is supported for multiple-display support. Confirm that you have the most current drivers (that are Windows Vista–compliant and support dual-mode capabilities) loaded. Confirm that Windows Vista is able to detect the secondary video adapter. Try selecting the secondary adapter rather than the primary adapter in the Display Settings dialog box.

No output appears on the secondary display. Confirm that your secondary adapter is supported for multiple-display support, especially if you are using a built-in motherboard video adapter. Confirm that the correct video driver has been installed for the secondary display. Restart the computer to see if the secondary video driver is initialized. Check the status of the video adapter in Device Manager. Try switching the order of the video adapters in the computer's slots. See if the system will recognize the device as the primary display.

An application is not properly displayed. Disable the secondary display to determine if the problem is specific to multiple-display support. Run the application on the primary display. If you are running MS-DOS applications, try running the application in full-screen mode. For Windows applications, try running the application in a maximized window.

Power Management for Mobile Computer Hardware

Windows Vista includes several features that are particularly useful for laptop computers. For example, through Power Options in Control Panel (found in the System and Maintenance section), you can select a power plan and enable power-management features with Windows Vista.

In the following sections, you will learn about improvements to power management, how to manage power states, how to manage power options, and how to troubleshoot power management.

Recognizing the Improvements to Power Management

Windows Vista builds upon the power-management features that were introduced with Windows 2000 and Windows XP with the following enhancements:

- Battery meter, which provides a notification icon in the System Tray that details the computer's battery power
- Power plans, which are collections of hardware and software settings optimized for a specific function
- Sleep power state, which combines the speed of standby with the features of hibernate mode
- ReadyDrive, which provides faster booting and resume times when used in conjunction with ReadyDrive-capable hard drives

Managing Power States

In Windows Vista, the *Advanced Configuration Power Interface (ACPI)* specifies different levels of power states:

- Fully active PC
- Sleep
- Hibernation
- Complete shutdown of PC

The *sleep* power state is a new power state introduced with Windows Vista that combines the features of hibernate and standby. When a computer enters the sleep power state, data including window locations and running applications is saved to the hard disk, and that session is available within seconds when the computer wakes. This allows the computer to be put into a power-saving state when not in use but allows quick access to the in-process user session, which allows the user to begin working more quickly than if the computer were shut down or put into hibernation.

Hibernation falls short of a complete shutdown of the computer. With hibernation, the computer saves all of your Desktop state as well as any open files. To use the computer again, press the power button. The computer should start more quickly than from a complete shutdown because it does not have to go through the complete startup process. You will have to again log on to the computer. Similar to when the computer is put into sleep mode, all the documents that were open when the computer went into hibernation are still available. With hibernation you can easily resume work where you left off. You can configure your computer to hibernate through Power Options or by choosing Start, then clicking the arrow and selecting Hibernate from the drop-down menu. This option will appear only if hibernation has been enabled through Power Options.

Unless you want to completely shut down the computer, configuring the computer to enter sleep mode is typically the best power-saving option. You may need to upgrade your computer's BIOS in order to use advanced power modes, such as sleep.

Managing Power Options

You configure power options through the Power Options Properties dialog box, as shown in Figure 3.10. To access this dialog box, access Control Panel ➢ System and Maintenance ➢ Power Options. The Power Options dialog box provides the ability to manage power plans, and to control power options, such as when the display is turned off, when the computer sleeps and what the power button does.

Configuring Power Plans

Windows Vista includes three configurable power plans: Balanced, Power Saver, and High Performance. Power plans control the trade-off between quick access to an existing computer session and energy savings. In Windows Vista, each power plan contains default options that can be customized to meet the needs of various scenarios.

The *Balanced* power plan, as its name suggests, provides a balance between power savings and performance. By default, this plan is configured to turn off the display after 20 minutes, and to put the computer to sleep after one hour of idle time. These times can be modified as needed. Other power options that can be modified include Wireless Adapter settings and Multimedia settings. Wireless adapters can be configured for maximum power saving or maximum performance. By default, the Balanced power plan configures wireless adapters for maximum performance. The Multimedia settings can be configured so that the computer will not be put into sleep mode when sharing media from the computer. For example, if the computer is acting as a Media Center device, then you can configure the computer to remain on by setting the Prevent Idling to Sleep option so that other computers

can connect to it and stream media from it even when the computer is not being used for other purposes.

The *Power Saver* power plan is optimized for power savings. By default, the display is configured to be turned off after 20 minutes of inactivity, and the computer will be put into sleep mode after one hour of inactivity. Additionally, this power plan configures hard disks to be turned off after 20 minutes of inactivity.

The *High Performance* power plan is configured to provide the maximum performance for portable computers. By default, the computer will never enter sleep mode, but the display will be turned off after 20 minutes. When this setting is configured, by default, the Multimedia settings are configured with the Allow the Computer to Enter Away Mode option, which allows the computer to enter into a new power state called *away mode*. Away mode configures the computer to appear off to users but remain accessible for media sharing. For example, the computer can record television shows when in away mode.

You can modify the existing power plans to suit your needs by clicking Change Plan Settings or you can use the preconfigured power plans listed in Table 3.3.

FIGURE 3.10 The Power Options Properties dialog box

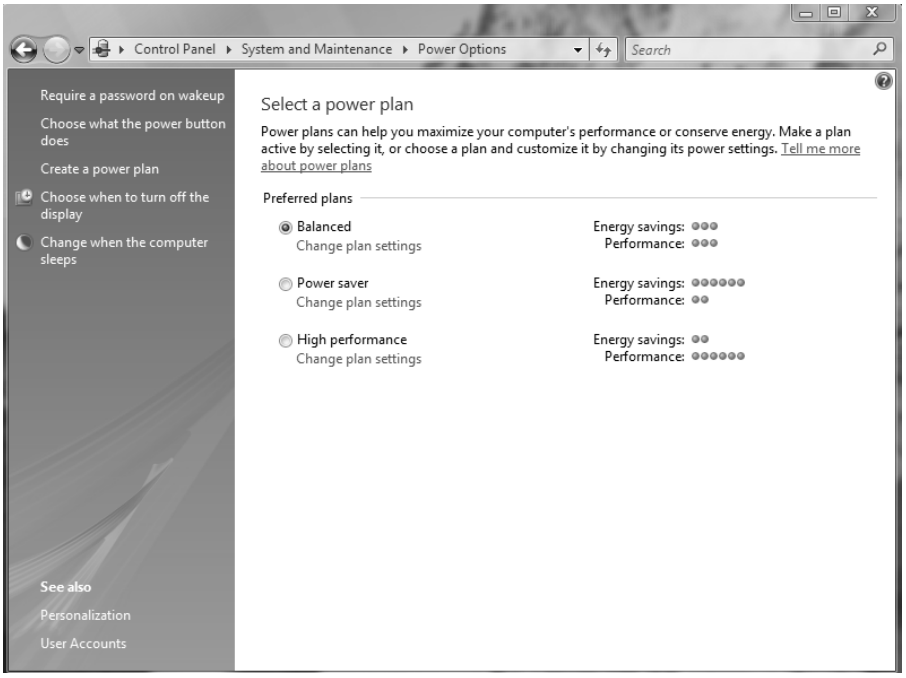


TABLE 3.3 Windows Vista Power Plans

Power Plan	Turn Off Display	Put The Computer To Sleep
Balanced	After 20 minutes	1 hour
Power Saver	After 20 minutes	1 hour
High Performance	After 20 minutes	Never

Configuring Advanced Power Settings

Each power plan contains advanced settings that can be configured, such as when the hard disks will be turned off and whether a password is required on wakeup. To configure these advanced settings, you click Control Panel ➢ System and Maintenance ➢ Power Options and select the power plan to use. You then click Change Advanced Power Settings to open the Advanced Settings tab of the Power Options dialog box, as shown in Figure 3.11. You can then modify the settings as desired or restore the plan defaults. For example, one option that you might want to change if you are using a mobile computer is the Power Buttons and Lid option, which configures what happens when you press the power button or close the lid of the mobile computer. When either of these actions occurs, the computer can be configured to do nothing, shut down, go into sleep mode, or go into hibernate mode.

FIGURE 3.11 Advanced Power Settings

Configuring Hibernation

Although sleep is the preferred power-saving mode in Windows Vista, hibernation is still available for use. Hibernation for a computer means that anything stored in memory is also stored on your hard disk. This ensures that when your computer is shut down, you do not lose any of the information that is stored in memory. When you take your computer out of hibernation, it returns to its previous state.

To configure your computer to hibernate, access the Advanced Settings tab of the Power Options dialog box by clicking Control Panel ➢ System and Maintenance ➢ Power Options, selecting the power plan to use, and clicking Change Advanced Power Settings. The Hibernate option appears under the Sleep option.

In Exercise 3.5, you configure a power plan for your computer.

EXERCISE 3.5

Configuring Power Plan Options

1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Power Options icon.
2. Select a power plan to modify from the Preferred Plans list and click Change Plan Settings, or select Create a Power Plan to create a new power plan.
3. Configure the power plan options for your computer based on your personal preferences. Click Change Advanced Power Settings to modify advanced power settings. When all changes have been made, click Save Changes.
4. Close Control Panel.

Managing Power Consumption Using the Battery Meter

Windows Vista includes a battery meter that you can use to monitor the battery power consumption on your computer. The battery meter also provides notification on what power plan is being used.

The battery meter appears in the notification area of the Windows taskbar and indicates the status of the battery, including the percentage of battery charge. As the battery charge gets lower, the battery meter provides a visual indication of the amount of charge left. For example, when the battery charge reaches the low-battery level, a red circle with a white X is displayed.

The battery meter also provides a quick method for changing the power plan in use on the computer. By clicking the battery meter icon, you can select between the three preferred power plans available with Windows Vista.

Using Windows ReadyBoost and Windows Vista

With Windows Vista, Microsoft has introduced several new technologies to help boost operating system performance. Windows ReadyBoost is a new technology introduced with Windows

Vista that allows for the use of nonvolatile flash memory devices as an additional memory cache. When the physical memory devices become full on a computer with Windows ReadyBoost configured, data is written to the flash device instead of to the hard drive. This improves performance because data can be read more quickly from the flash drive than from the hard drive. When a compatible device is installed on a Windows Vista computer, a ReadyBoost tab is displayed on the device's properties page that can be used to configure Windows ReadyBoost.

To use a flash memory device with Windows ReadyBoost, the device must meet the following specifications:

- The device must have a storage capacity of at least 256MB.
- The device must support USB 2.0.
- The device must support a throughput of 2.5MB/sec for 4K random reads and 1.75MB/sec for 512K random writes.

Using ReadyDrive and Windows Vista

ReadyDrive is a new technology included with Windows Vista that you can use to speed up the boot process, resume from a hibernation state faster, and conserve battery power for mobile computers. ReadyDrive relies on new hybrid hard disks, which use flash memory technology in conjunction with mechanical hard disk technology.

When you use ReadyDrive, data is written to flash memory instead of to the mechanical hard disk. This saves battery power because the mechanical hard disk does not need to perform as many read/write actions. Additionally, read/write times with flash memory is quicker than with traditional hard disk media, so resuming from hibernation occurs faster.

Managing I/O Devices

Your input/output (I/O) devices are the ones that allow you to get information into and out of your computer. Examples of I/O devices are keyboards, mice, printers, and scanners. Your devices may be connected to your computer by standard cabling, or they may use wireless technology (such as IrDA or RF) or be connected through a USB port.

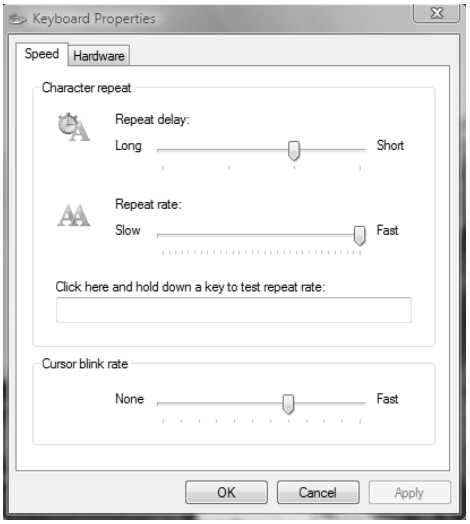
The following sections describe how to manage your keyboard, mouse, wireless devices, and USB devices.

Configuring the Keyboard

Most of the time, you can leave the keyboard settings at default values. However, if needed you can configure advanced keyboard options.

You can configure keyboard options through the Keyboard Properties dialog box, shown in Figure 3.12. To access this dialog box, open Control Panel, then Hardware and Sound, and then click Keyboard.

FIGURE 3.12 The Keyboard Properties dialog box



You must have a keyboard attached to your computer before you can install Windows Vista.

This dialog box has two tabs with options that control your keyboard's behavior:

- The Speed tab lets you configure how quickly characters are repeated when you hold down a key. You can also specify the cursor blink rate.
- The Hardware tab specifies the device settings for your keyboard.

Configuring the Mouse

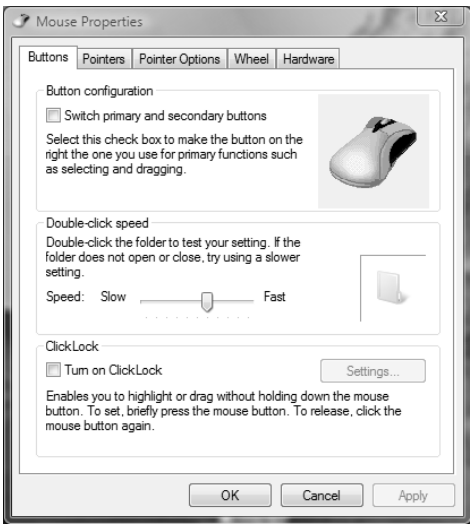
You can configure your mouse through the Mouse Properties dialog box, shown in Figure 3.13. To access this dialog box, open Control Panel, then click Hardware and Sound, and then select the Mouse option.

The Mouse Properties dialog box has five tabs with options that control your mouse's behavior:

Buttons Allows you to configure the mouse properties for right-handed or left-handed use. You can also configure the speed that is used to indicate a double-click. The ClickLock option is used to highlight and drag a selection without holding down the mouse button while the object is being moved. ClickLock is not enabled by default.

Pointers Lets you select a predefined pointer scheme that is used by your mouse, for example, Conductor (system scheme), which uses music-themed pointers. You can also create custom pointer schemes.

FIGURE 3.13 The Mouse Properties dialog box



Pointer Options Lets you specify how fast your mouse pointer moves. You can also configure the Snap To feature, which automatically moves the pointer to a default button in a dialog box when new dialog boxes are opened. Visibility options are used to configure if pointer trails are displayed, if the pointer is hidden while typing, and whether the location of the pointer is shown when the Ctrl key is pressed.

Wheel Configures how many vertical lines are scrolled when the wheel is rolled. You can also configure horizontal scrolling if a tilt-wheel mouse is used.

Hardware Specifies the device settings for your mouse.

In Exercise 3.6, you will configure your keyboard and mouse I/O devices.

EXERCISE 3.6

Configuring I/O Devices

1. Select Start ➢ Control Panel ➢ Hardware and Sound ➢ Keyboard.
2. On the Speed tab, set the Repeat Delay and Repeat Rate options based on your personal preferences. Also adjust the Cursor Blink Rate if you want to change it. Click OK.
3. In Control Panel, Hardware and Sound, click Mouse.
4. In the Pointer Options tab, set the Motion and Snap-To options as you prefer. Click OK.
5. Close Control Panel.

Configuring Handwriting Recognition

Another method of inputting information into a computer is through handwriting recognition. The Tablet PC provides the ability to write using a stylus instead of typing using the keyboard. The Tablet PC Input Panel allows you to enter text into a writing pad, and the text is then converted into typed text. Other applications written for the Tablet PC also allow for the use of handwriting text instead of requiring the use of the keyboard.

In some cases, the handwriting recognizer does not properly recognize your handwriting. The Handwriting recognition personalization tool allows you to provide samples of your writing that can be used to train the handwriting recognizer. You can access the Handwriting recognition personalization tool by opening the Tablet PC Input Panel, tapping Tools, then tapping Personalize Handwriting Recognition.

Configuring Wireless Devices

Wireless devices use wireless transmission rather than transmitting over cable. Windows Vista supports IEEE 802.11–compatible devices. IEEE 802.11 is an industry standard for wireless support. Windows Vista also supports Bluetooth, which is a short-range radio technology that simplifies communication between local computer devices and Internet devices.

The following are two of the technologies used for wireless transmission:

- Infrared Data Association (IrDA), which is a standard for transmitting data through infrared light waves
- RF (Radio Frequency), which is a standard for transmitting data through radio waves

Common examples of wireless devices include keyboards, mice, and network cards. You should follow the vendor's instructions to install wireless devices. Wireless devices are configured in the same manner as other devices on your computer. For example, you can set options for a wireless keyboard through the Keyboard Properties dialog box.

Windows Vista also supports connecting devices, such as Windows Mobile phones, personal digital assistants (PDAs) and printers, using Bluetooth technology. If your computer is equipped with a Bluetooth adapter, you can connect a Bluetooth device to your computer by performing the following steps:

1. Turn the device on, and ensure that it can be accessed from other devices.
2. Click Start ➢ Control Panel ➢ Hardware and Sound ➢ Bluetooth Devices.
3. Click Add to add the device to the computer.
4. Click the Options tab, and ensure that the Allow Bluetooth Devices to Connect to This Computer option is enabled.

If you are synchronizing data wirelessly between your computer and a Bluetooth device, you can view the status of the synchronization and any conflicts by accessing the Sync Center by clicking Control Panel ➢ Network and Internet ➢ Sync Center.

Managing USB Devices

Universal Serial Bus (USB) is an external bus standard that allows you to connect USB devices through a USB port. USB supports transfer rates up to 480Mbps. A single USB port can support up to 127 devices. Examples of USB devices include flash memory devices, printers, and keyboards.

Configuring USB Devices

If your computer supports USB, and USB is enabled in the BIOS, you will see Universal Serial Bus controllers listed in Device Manager. Double-click your USB controller to see the dialog box shown in Figure 3.14.

The USB controller Properties dialog box has at least four tabs (depending on your driver, you might have additional tabs, for example, Details) with options and information for your USB adapter:

General Lists the device type, manufacturer, and location. It also shows the device status, which indicates whether the device is working properly. If the device is not working properly, you can click the Troubleshoot button in the lower-right area of the dialog box.

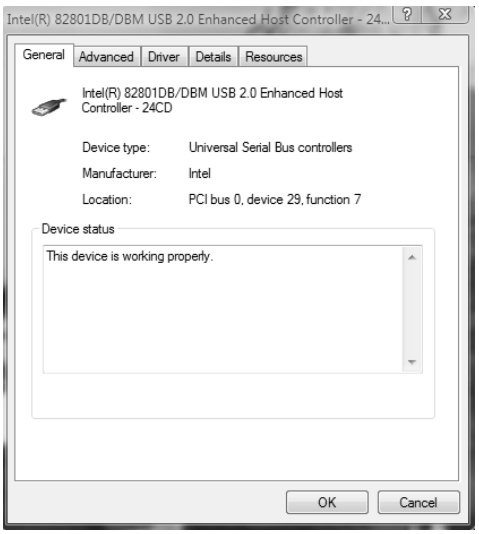
Advanced Allows you to configure how much of the bandwidth each device that is connected to the USB adapter can use.

Driver Shows driver properties and lets you uninstall or update the driver.

Resources Shows all of the resources that are used by the USB adapter.

After the USB adapter is configured, you can attach USB devices to the adapter in a daisy-chain configuration.

FIGURE 3.14 The USB controller Properties dialog box



Troubleshooting USB

Some of the errors you may encounter with USB and the associated fixes are as follows:

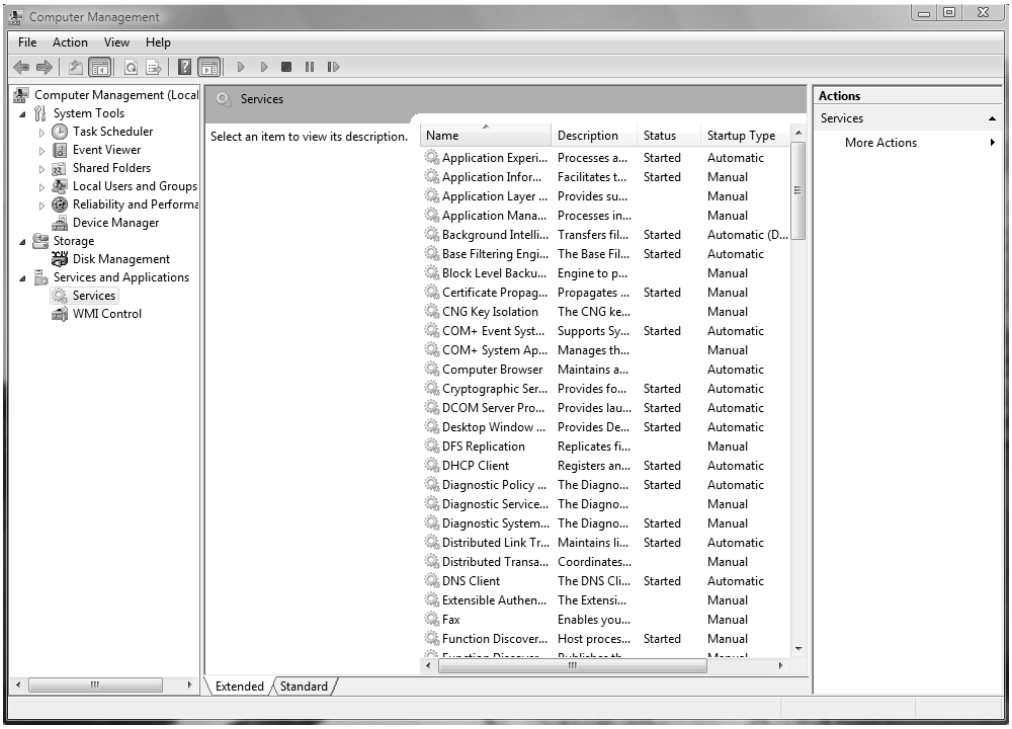
- Your USB driver may be corrupted or not properly installed. Uninstall the device driver and rescan your computer for new hardware to let Windows Vista detect and install the proper driver for your device.
- You may have malfunctioning or incorrectly configured USB hardware. If you suspect that this is the case, and you have another computer running USB, you should try to run the USB hardware on the alternate computer. You should also check the status of the device in Device Manager. To support USB, the computer must have an IRQ assigned for the root USB controller in the computer's BIOS.
- You may have mismatched cabling. USB supports two standards: high-speed and low-speed. Make sure the cables are the proper type for your configuration.
- Make sure your BIOS and firmware are up-to-date. If the BIOS or firmware is not compatible with USB, you may see multiple instances of your device in Device Manager with no associated drivers for the multiple instances.
- The root hub may be improperly configured. USB controllers require that an IRQ be assigned in the computer's BIOS. If the controller is not properly configured, you will see the root hub displayed in Device Manager with a yellow exclamation point.
- If you are using a USB bus-powered hub, the device attached to the hub may require more power than the hub can provide. In this case you should use a self-powered USB hub. You can determine if the hub is the problem by removing the hub and directly attaching the device to the computer's USB. You can also troubleshoot this error by attaching the device to a self-powered USB hub and seeing if it works.

If your computer has a built-in USB device and does not detect the device through Device Manager, confirm that the USB is enabled in the computer's BIOS and that the BIOS supports USB devices.

Managing Windows Vista Services

A service is a program, routine, or process that performs a specific function within the Windows Vista operating system. You can manage services through the Services window (Figure 3.15), which can be accessed in a variety of ways. If you go through the Computer Management utility, right-click Computer, select Manage, expand Services and Applications, and then expand Services. You can also go through Administrative Tools or set up Services as an MMC snap-in.

FIGURE 3.15 The Services window



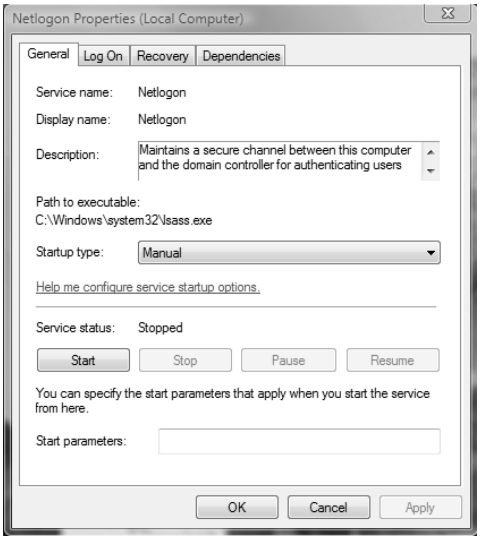
For each service, the Services window lists the name, a short description, the status, the startup type, and the logon account that is used to start the service. To configure the properties of a service, double-click it to open its Properties dialog box, shown in Figure 3.16. This dialog box contains four tabs of options for services: General, Log On, Recovery, and Dependencies.

General Allows you to view and configure the following options:

- The service display name
- A description of the service
- The path to the service executable
- The startup type, which can be automatic, manual, or disabled
- The current service status
- Start parameters that can be applied when the service is started

In addition, the buttons across the lower part of the dialog box allow you change the service status to start, stop, pause, or resume the service.

FIGURE 3.16 The Properties dialog box for a service



Log On The Log On tab, shown in Figure 3.17, allows you to configure the logon account that will be used to start the service. Choose the local system account or specify another logon account. At the bottom, you can select hardware profiles with which to associate the service. For each hardware profile, you can set the service as enabled or disabled.

Recovery The Recovery tab, shown in Figure 3.18, allows you to designate what action will be taken if the service fails to load. For the first, second, and subsequent failures, you can select from the following actions:

- Take No Action
- Restart the Service
- Run a Program
- Restart the Computer

If you choose Run a Program, specify it along with any command-line parameters. If you choose Restart the Computer, you can configure a message that will be sent to users who are connected to the computer before it is restarted.

Dependencies The Dependencies tab, shown in Figure 3.19, lists any services that must be running in order for the specified service to start. If a service fails to start, you can use this information to examine the dependencies and then make sure each one is running. In the bottom panel, you can verify whether any other services depend on this service before you decide to stop it.

FIGURE 3.17 The Log On tab of a service's Properties dialog box

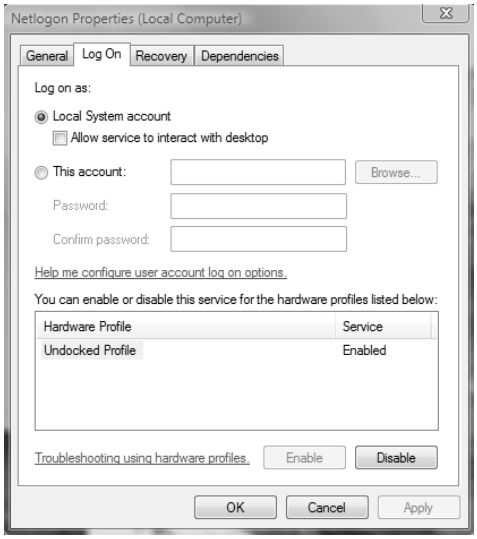


FIGURE 3.18 The Recovery tab of a service's Properties dialog box

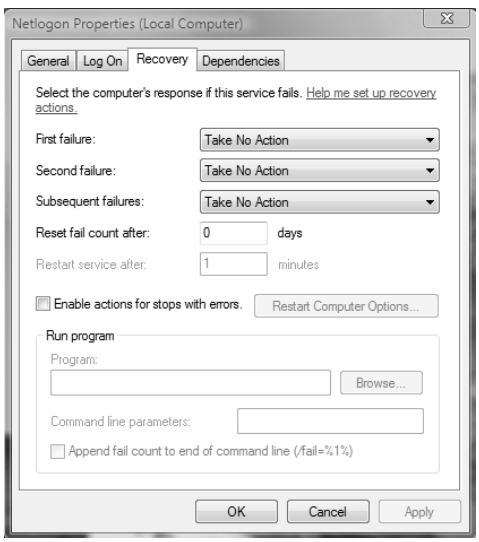
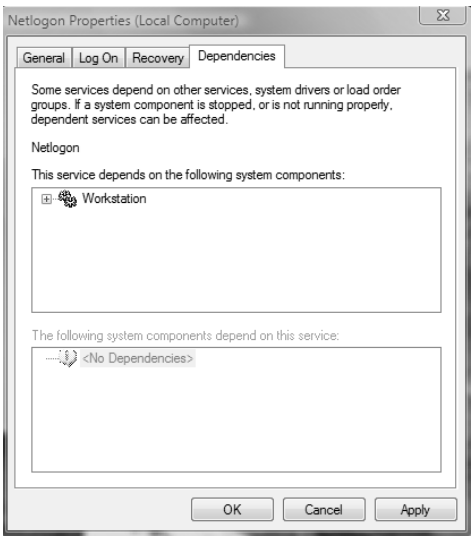


FIGURE 3.19 The Dependencies tab of a service's Properties dialog box



Summary

In this chapter, you learned about configuring the Windows Vista environment. We covered the following topics:

- New enhancements to Windows Vista configuration and support
- Utilities used to manage configuration, which include the Microsoft Management Console (MMC) and the Registry Editor
- Installing hardware, including Plug and Play and non–Plug and Play devices
- Managing device drivers, including how to update and reinstall drivers
- Managing disk devices, including CD-ROM devices, DVD devices, and removable media
- Managing display devices, including video adapters and multiple displays
- Managing mobile computer hardware, including how to configure power plans
- Managing I/O devices, including keyboards, mice, wireless devices, and USB devices
- Managing imaging devices, including scanners and digital cameras
- Managing Windows Vista services
- Enhancing performance using Windows ReadyBoost and Windows ReadyDrive

Exam Essentials

Understand how to install new hardware on your computer. Be able to successfully install hardware that is Plug and Play compatible, as well as hardware that is not Plug and Play compatible.

Know how to manage and update device drivers. Be able to successfully upgrade device drivers. Be able to roll back drivers to a previously known-good state.

Know how to manage display devices. Understand how to configure your computer with a single monitor or multiple monitors. Be able to list the requirements for installing and configuring multiple monitors.

Be able to support mobile computers through power management features. Understand the new power features that are available Windows Vista and be able to configure a laptop computer to use these features.

Be able to enhance Windows Vista performance. Understand the new performance enhancement features of Windows Vista. Know when to use these features.

Review Questions

1. You are the system administrator for your company. You are configuring the services on a Windows Vista computer. You want to ensure that if a service fails to load, it will attempt to restart. Which tab of the service's Properties dialog box should you use?

   A. General

   B. Log On

   C. Recovery

   D. Dependencies

2. The system administrator of the XYZ network wants to edit the Registry, including setting security on the Registry keys. What primary utility that supports full editing of the Windows Vista Registry should the system administrator use?

   A. REGEDIT

   B. REDIT

   C. REGEDIT32

   D. REGEDITOR

3. Jim has an XYZ-manufactured sound card installed in his computer. The XYZ Corporation released a new driver for the card. Jim is slightly worried that the driver may not have been fully tested and may cause his computer to work improperly. What is the process that Microsoft uses with Windows Vista to ensure that the drivers you install on your computer are properly tested and verified?

   A. Driver confirmation

   B. Driver optimization

   C. Driver signing

   D. Driver verification

4. Tracey is the network administrator for a large company. One of her users wants to set up a dual-monitor work area for her Windows Vista computer. Which of the following statements is true regarding configuration of multiple displays?

   A. You need a special cable that allows you to connect two monitors to a video adapter.

   B. You can install an adapter for each monitor that you will configure.

   C. You must use a PCI-Express video adapter.

   D. Windows Vista allows you to extend your Desktop across up to eight monitors.

5. A member of your company's sales group has attached a USB camera to their Windows Vista computer. The sales employee indicated that she manually installed the driver for the camera with a driver that she downloaded from the Internet. The camera is shown in Device Manager, but the camera is not functioning. You need to troubleshoot the camera so that it can communicate with the computer. Which of the following should you do?

   A. Disconnect the camera and then reconnect it.

   B. Reinstall the original driver.

   C. Uninstall the camera, disconnect it, and then reconnect it.

   D. Disable the device, disconnect it, and then reconnect it.

6. You are the network administrator for a small company. One of your users, Todd, has a new device that connects to his computer through either the serial port or the USB port. He attempts to connect the device to the USB port through a USB root hub, but the device is not recognized. You verify that all of the hardware is on the Hardware Compatibility List for Windows Vista and that you have the latest drivers. No other devices will connect to the USB root hub, and they also don't work. You verify that the USB root hub and USB device will work on another computer, which is running Windows XP and has USB configured. What is the next course of action you should take?

   A. Verify that an IRQ has been assigned to the USB controller in the computer's BIOS.

   B. Configure the Registry setting for `HKEY_LOCAL_COMPUTER\HARDWARE_DEVICES\USB` to 0.

   C. Configure the Registry setting for `HKEY_LOCAL_COMPUTER\HARDWARE_DEVICES\USB` to 1.

   D. Downgrade the drivers to Windows XP drivers and see if the device will work.

7. Tina is dissatisfied with the configuration of her keyboard and mouse. She wants to reset the keyboard speed and the mouse pointer rate. Which utility should she use to configure the keyboard and mouse properties?

   A. Control Panel

   B. Computer Management

   C. Microsoft Management Console

   D. Registry Editor

8. Miguel is trying to install a network card that is not Plug and Play compatible. When he restarts the computer, the card is not recognized. He has a Windows Vista driver for the device and wants to manually configure the network card. Which utility should he use to install the network card?

   A. Device Manager

   B. Computer Manager

   C. Control Panel (Classic View), Add Hardware utility

   D. MMC

9. Elena is using a laptop computer that uses ACPI. She wants to see what percentage of the battery power is still available. She also wants to know if hibernation has been configured. Which of the following utilities should she use?

   A. Device Manager

   B. Computer Manager

   C. Battery meter

   D. MMC

10. Fred has configured his wireless phone to synchronize with his computer using Bluetooth technology. However, Fred realizes that an error occurs while synchronizing the device and the data was not copied to his computer. He wants to view the conflict and attempt to resolve it, if possible. Which utility should he use to view synchronization conflicts?

    A. Device Manager

    B. Computer Manager

    C. Sync Center

    D. MMC

11. You are administering a computer that is used by several customer support representatives for your company. The support representatives use a custom application to report support incidents. After updating the application, it stops functioning properly, and one of the programmers who wrote the application indicates that a Registry change needs to be made to the computer. You need to ensure that the change is applied for each user of the computer. Which Registry key should you modify?

    A. `HKEY_CLASSES_ROOT`

    B. `HKEY_CURRENT_USER`

    C. `HKEY_LOCAL_MACHINE`

    D. `HKEY_USERS`

12. Jose has received a Windows Vista laptop from work; it was originally licensed to Joe Smith. He wants to change that name to Jose Gonzales. He wants to change the value of this specification within the Registry but doesn't know the name of the key that is used to set the license name. What command should Jose use to change the licensing information through the Registry?

    A. REGEDIT

    B. REDIT

    C. REGEDIT32

    D. EDTREG32

13. You have a user, Bob, who uses a laptop computer running Windows Vista. You have configured the laptop to enter sleep mode after 20 minutes of inactivity. What will occur when the computer enters sleep mode?

A. The data will be saved to the hard disk, and the computer will shut down.

B. The data will be erased from RAM, and the computer will shut down.

C. The monitor will be turned off, but the hard disks will remain active.

D. The data will be saved to the hard disk, and the computer will be put into a power-saving state.

14. You have created a new MMC that will be used on a Windows Vista computer that is used by several people. You want to ensure that users can access each item in the console tree, but you do not want other users to be able to add new snap-ins to the MMC. Which console mode option should you configure for the MMC?

A. Author Mode

B. User Mode – Full Access

C. User Mode – Limited Access, Multiple Window

D. User Mode – Limited Access, Single Window

15. You have configured your computer for multiple-display support. Everything works properly when you run Windows applications. However, you do not see your MS-DOS application properly displayed. What can you do?

A. Try running the application in full-screen mode.

B. Restart the computer and see if the secondary video adapter is initialized.

C. Increase the screen area on both displays to 1024×768.

D. Set the Colors option to Medium (16 bit).

16. You want to configure your Windows Vista laptop computer so that the display is turned off after 20 minutes, but you do not want the computer to shut down completely. You want to use one of the preconfigured power plans. Which power plan should you use?

A. Balanced

B. Power Saver

C. High Performance

D. Power Balance

17. You want to speed up the resume time on your computer after it is put into hibernate mode. You have installed a hybrid hard disk drive into your Windows Vista computer. Which technology should you use to accomplish your goal?

A. ReadyDrive

B. ReadyBoost

C. Superfetch

D. SuperDrive

18. A new employee named Sue has been supplied with a Windows Vista laptop computer. You have configured Sue's computer with the Power Saver power plan, and you used the default options. Which of the following will occur after 30 minutes of inactivity on Sue's computer?

A. The display will be turned off, but the hard disk will remain active.

B. The hard disk will be turned off, but the display will remain active.

C. Both the hard disk and the display will be turned off.

D. No components will be turned off.

19. You have installed a new driver for the video adapter on a Windows Vista computer. However, the video on the computer is no longer functioning properly, and you want to roll back the driver. Which management utility should you use?

A. Device Manager

B. Control Panel

C. MMC

D. Registry Editor

20. You are configuring a laptop computer running Windows Vista. You want to ensure that after a specified period of inactivity the computer is put into a power saving state. However, you want to ensure that data is saved to the hard disk, that the computer is quickly accessible on wakeup, and that the computer is never shut down. Which power-saving mode should you configure?

A. Standby mode

B. Sleep mode

C. Hibernate mode

D. Hybrid mode

Answers to Review Questions

1. C. You can configure what actions will occur if the service fails to start on the Recovery tab of the service's Properties dialog box. For example, you can configure the service to attempt to restart, or you can configure the computer to reboot.

2. A. In Windows Vista, you can edit the Registry with REGEDIT or REGEDT32. You should always use extreme caution when editing the Registry, as improper configurations can cause the computer to fail to boot.

3. C. Microsoft uses driver signing to verify that drivers have been properly tested before they are installed on a Windows Vista computer.

4. B. If you want to configure multiple displays in Windows Vista, you can install multiple adapters or a single adapter that supports multiple monitors. You can use PCI or AGP video adapters in addition to PCI-Express video adapters. Windows Vista allows you to extend your Desktop across more than eight monitors.

5. C. You should uninstall the camera, disconnect it from the computer, and then reconnect it. Doing so will uninstall the driver that was manually installed, and when the camera is reconnected, the operating system will scan for a suitable driver for the device and install that driver.

6. A. The root hub may be improperly configured. USB controllers require that an IRQ be assigned in the computer's BIOS. If the controller is not properly configured, you will see the root hub displayed in Device Manager with a yellow exclamation point.

7. A. You configure keyboard and mouse properties in Control Panel.

8. C. The Add Hardware utility in Control Panel (Classic View) starts the Add Hardware Wizard to install hardware that is not Plug and Play compatible. You need to verify that other devices do not already use the configuration settings that you select for resource use.

9. C. On a laptop computer, Elena can use the battery meter to view the amount of battery power available and to change the power plan configured for the computer.

10. C. You can use the Sync Center to view conflicts that occurred during the synchronization process. To access the Sync Center, click the Start button, click Control Panel, click Network and Internet, then click Sync Center. Conflicts can be viewed by clicking View Sync Conflicts in the Sync Center.

11. C. You will need to make the Registry modification in the `HKEY_LOCAL_MACHINE` Registry key. This key provides configuration information that is accessible regardless of who is logged onto the computer.

12. A. In Windows Vista, you can edit the Registry with REGEDIT or REGEDT32. You should always use extreme caution when editing the Registry, as improper configurations can cause the computer to fail to boot.

13. D. When the computer enters sleep mode, the data will be saved to the hard disk, and the computer will be put into a power-saving state. Sleep mode combines the features of standby and hibernate so that all data is saved to the hard disk, but the computer restores faster than if the computer were put into hibernate mode.

14. B. You should configure the User Mode – Full Access console mode for the MMC. This mode allows users to fully access the MMC console tree, but they will be unable to add or remove snap-ins from the MMC.

15. A. If you are running an MS-DOS application with multiple-display support and you do not see the application properly, try running the application in full-screen mode. If the problem is occurring with a Windows application, try running the application in a maximized window. You could also try disabling the secondary display to determine whether the problem was specific to multiple-display support.

16. C. You should configure the High Performance power plan on your Windows Vista laptop computer. The High Performance power plan configures the display to shut down after 20 minutes by default, but the computer is never put to sleep. You can also customize any of the available power plans or create a new one. To configure power plan options, access the Control Panel, click System and Maintenance, and select Power Options.

17. A. You should use the Windows ReadyDrive technology to help speed the resume time of your computer after it has been put into hibernate mode. ReadyDrive is a new technology that is used in conjunction with hybrid hard disk drives, which combine flash memory with standard hard disk technology. This allows data to be stored in flash memory, which enables the hard disk to remain spun down longer and also improves the time required for the computer to resume after being put into hibernate mode.

18. C. When a Windows Vista computer is configured with the Power Saver power plan, the computer's display and hard disk will be turned off after 20 minutes of inactivity in order to conserve energy. The computer will be put into sleep mode after one hour of inactivity when using the Power Saver power plan.

19. A. To roll back a driver to a previous state, you should use Device Manager. In Device Manager, you can view driver information for an installed device, and you can update the driver or roll it back to a previous state.

20. B. To ensure that data is saved to the hard disk, that the computer is quickly accessible on wakeup, and that the computer is never shut down when put into a power-saving state, you should configure the computer to use sleep mode. Sleep mode is a combination of standby mode and hibernate mode. The user's session is quickly accessible on wakeup, but the data is saved to the hard disk. Sleep mode is the preferred power-saving mode in Windows Vista.

Chapter

4

Configuring the Windows Vista Desktop

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring and Troubleshooting Post-Installation System Settings**
  - Troubleshoot post-installation configuration issues
  - Configure and troubleshoot Windows Aero
- ✓ **Configuring Applications Included with Windows Vista**
  - Configure Windows Sidebar

Windows Vista offers many options for configuring the Desktop to suit personal preferences. These options include customizing the taskbar and Start Menu, creating shortcuts, setting display properties, and configuring Windows Sidebar.

Because of Windows Vista's modular architecture, support for multiple languages and regional settings is improved over previous versions. The support that comes with localized editions of Windows Vista allows users to view, edit, and print multilingual documents, which can include documents that are written in almost any language. You can also specify locale settings for the Desktop to customize items such as the date format and currency for your geographical location.

The accessibility options support users with limited sight, hearing, or mobility. You can configure the Desktop and use Windows Vista utilities to provide a higher degree of accessibility.

This chapter describes how to manage Desktop settings, multilanguage support, and accessibility options.

Configuring Desktop Settings

You can set Windows Vista to use the Windows Vista Aero theme, the Windows Vista Standard theme, the Windows Vista Basic theme, the Windows Classic theme, or any customized theme you want. The Windows Vista *Desktop*, shown in Figure 4.1, appears after a user has logged on to a Windows Vista computer. Users can configure their Desktops to suit their personal preferences and to work more efficiently.

If you have installed Windows Vista from a clean install, you will notice that the Desktop is clean, with all the options for managing the computer grouped accessible from the Start Menu.

Table 4.1 lists the common options that appear on the Start Menu.

FIGURE 4.1 The Windows Vista Desktop

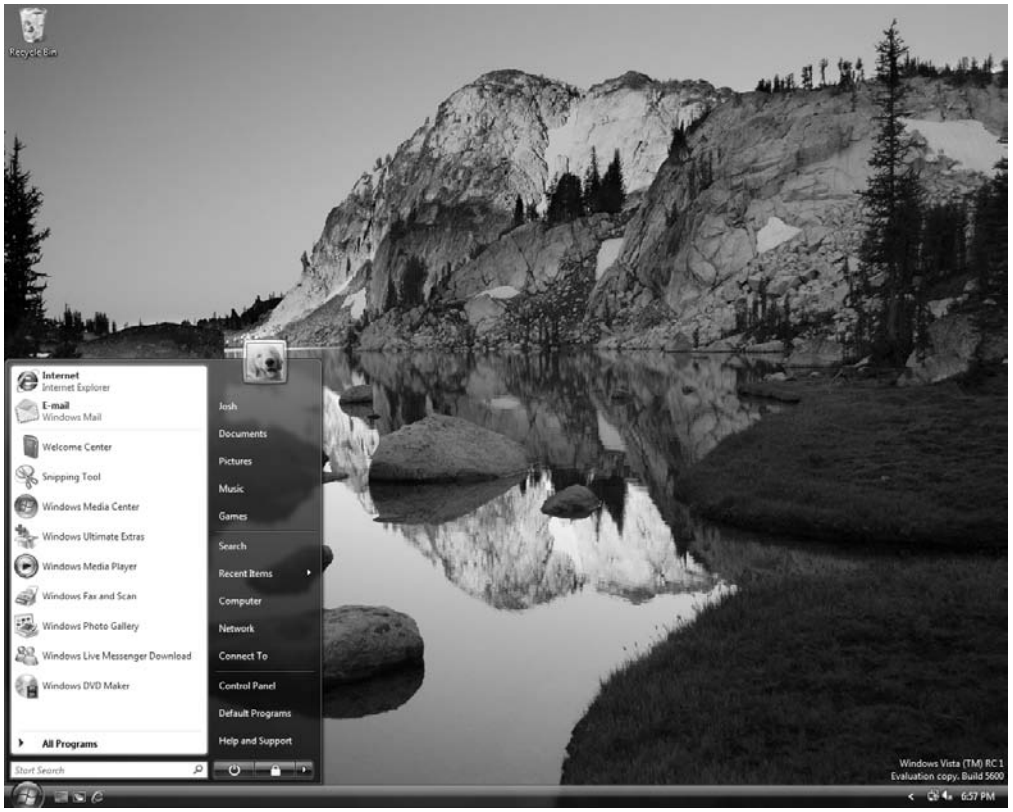


TABLE 4.1 Default Start Menu Items

Item	Description
Internet (Internet Explorer)	The built-in web browser. When used with an Internet connection, Internet Explorer (IE) provides an interface for accessing the Internet or a local intranet.
E-mail (Windows Mail)	Starts the default e-mail application, Windows Mail.

TABLE 4.1 Default Start Menu Items *(continued)*

Item	Description
Windows Media Player	Used to play multimedia files.
Windows DVD Maker	Used to view and edit photo and video files to create a DVD.
Windows Photo Gallery	Used to view and organize photos.
Documents	By default, stores the documents that are created. Each user has a unique Documents folder, so even if a computer is shared, each user will have unique personal folders.
Recent Items	Lists the documents you have recently accessed.
Pictures	Shows any pictures that are in the user's Pictures folder.
Music	Shows any music that is in the My Music folder.
Computer	Allows you to centrally manage your computer's files, hard drives, and devices with removable storage. Also allows you to manage system tasks and other places (such as other computers on the network) and to view details about your computer.
Control Panel	Allows you to configure your computer.
Windows Fax and Scan	Used to create and manage scan and fax resources.
Help and Support	Used to access Windows Vista Help and Support resources.
Search	Searches for pictures, music, video, documents, files and folders, computers, or people.
Power Button	Used to shut down the computer or place it into a low power state.

If you use any kind of remote management tools, you may want to rename the Computer icon to the actual computer's name. This allows you to easily identify which computer you're accessing.

To switch between themes, right-click an area of open space on the Desktop, select Personalize, and then click Theme. In the Theme Settings dialog box, you can then select the theme you want to use from the Theme pull-down menu.

You can configure the Desktop by customizing the taskbar and Start Menu, adding shortcuts, and setting display properties. We describe these configurations in the following sections.

The Desktop also includes the *Recycle Bin*. The Recycle Bin is a special folder that holds the files and folders that have been deleted, assuming that your hard drive has enough free space to hold the deleted files. If the hard drive is running out of disk space, the files that were deleted first will be copied over. You can retrieve and clear files (for permanent deletion) from the Recycle Bin.

Configuring Windows Aero

Windows Aero is the new user interface component of Windows Vista. When the Windows Aero theme is configured, open windows are displayed with a transparent glass effect and subtle animations.

Enabling Windows Aero on a computer that has less than 1GB of random access memory (RAM) and less than 128MB of video RAM could adversely affect the performance of the computer. Ensure that your computer meets the minimum requirements before enabling Windows Aero. Windows Vista minimum requirements are discussed in detail in Chapter 1, "Getting Started with Windows Vista."

To enable Windows Aero, you must first ensure that the Windows Vista theme is selected. This can be accomplished through the Personalization Control Panel option. Open this Control Panel option by right-clicking the Desktop, selecting Personalize, and then configure the Windows Vista theme by clicking Theme, then selecting Windows Vista from the Theme drop-down list. After the Windows Vista theme is configured, you will need to configure Windows Aero as the color scheme. To configure the Windows Aero color scheme, you should open the Personalization Control Panel option, select Window Color and Appearance to open the Appearance Settings dialog box, and select the Windows Aero option in the Color Scheme list. The Desktop changes to use the Windows Aero interface.

Once the Windows Aero color scheme is configured, clicking Window Color and Appearance will not display the Appearance Settings dialog box. Instead, the Window Color and Appearance dialog box will be displayed, which allows you to configure the color and transparency of the windows. To view the full transparent glass effect of Windows Aero, you should enable the Enable Transparency option of the Window Color and Appearance dialog box.

Customizing the Taskbar and Start Menu

Users can customize the *taskbar* and *Start Menu* through the Taskbar and Start Menu Properties dialog box, shown in Figure 4.2. The easiest way to access this dialog box is to right-click a blank area in the taskbar and choose Properties from the context menu.

The Taskbar and Start Menu Properties dialog box has four tabs: Taskbar, Start Menu, Notification Area, and Toolbars, containing the options described in the following sections.

FIGURE 4.2 The Taskbar tab of the Taskbar and Start Menu Properties dialog box

Configuring Taskbar Properties

Through the Taskbar tab of the Taskbar and Start Menu Properties dialog box (shown in Figure 4.2), you can specify taskbar and Start Menu features, such as whether the taskbar is always visible and whether window thumbnails should be shown. Table 4.2 lists the properties on the Taskbar tab.

TABLE 4.2 Taskbar Properties

Property	Description
Lock the Taskbar	Locks the taskbar into the current position so it cannot be moved around the Desktop and locks the size of the taskbar. This option is enabled by default.
Auto-Hide the Taskbar	Hides the taskbar. This option is disabled by default. When it is enabled, you show the taskbar by clicking the area of the screen where the taskbar appears.
Keep the Taskbar on Top of Other Windows	Keeps the taskbar visible, even if you open full-screen applications. This option is enabled by default.
Group Similar Taskbar Buttons	Keeps all taskbar buttons for the same program in the same location. Also specifies that if you have many applications open and the taskbar becomes crowded, all the buttons for a single application should be collapsed into a single button. This option is enabled by default.

TABLE 4.2 Taskbar Properties *(continued)*

Property	Description
Show Quick Launch	Shows the Quick Launch icon on the taskbar. Quick Launch lets you get back to the Windows Desktop with a single click. This option is enabled by default.
Show Window Previews (Thumbnails)	Displays a thumbnail preview of a window when the mouse is hovered over the taskbar icon.

Configuring Start Menu Properties

The Start Menu tab of the Taskbar and Start Menu Properties dialog box allows you to customize your Start Menu. By selecting Start Menu, you can customize the Windows Vista theme, or by selecting the Classic Start Menu option, you can use the look and feel of previous versions of Windows.

You can add or remove items from the Start Menu, remove records of recently accessed items, and specify which options are displayed by clicking the Customize button for the theme you want to use. Figure 4.3 shows the options for customizing the Start Menu for the Windows Vista theme.

The Customize Start Menu dialog box shows a list of options that you can enable or disable to change the look and feel of the Start Menu. Table 4.3 lists the options that you can configure using the Customize Start Menu dialog box.

FIGURE 4.3 Customize Start Menu dialog box

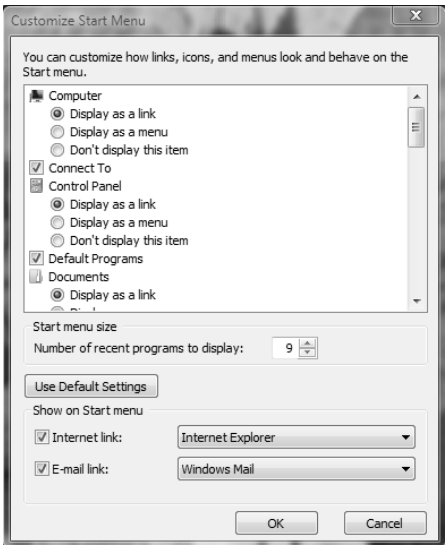


TABLE 4.3 The Start Menu Customizable Options

Option	Settings
Computer	The Computer icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Connect To	The Connect To option can be enabled or disabled.
Control Panel	The Control Panel icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Default Programs	The Default Programs option can be enabled or disabled.
Documents	The Documents icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Enable Context Menus and Dragging and Dropping	The Enable Context Menus and Dragging and Dropping option can be enabled or disabled.
Favorites Menu	The Favorites menu can be enabled or disabled.
Games	The Games icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Help	The Help option can be enabled or disabled.
Highlight Newly Installed Programs	The Highlight Newly Installed Programs option can be enabled or disabled.
Music	The Music icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Network	The Network option can be enabled or disabled.
Open Submenus When I Pause on Them with the Mouse Pointer	The Open Submenus When I Pause on Them with the Mouse Pointer option can be enabled or disabled.
Personal Folder	The Personal Folder icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Pictures	The Pictures icon can be configured to be displayed as a link, as a menu, or not displayed at all.
Printers	The Printers option can be enabled or disabled.

TABLE 4.3 The Start Menu Customizable Options *(continued)*

Option	Settings
Run command	The Run command option can be enabled or disabled.
Search	The Search option can be enabled or disabled.
Search Communications	The Search Communications option can be enabled or disabled.
Search Favorites and History	The Search Favorites and History option can be enabled or disabled.
Search Files	The Search Files icon can be configured to search the user's files, search the entire index, or to not search for files.
Search Programs	The Search Programs option can be enabled or disabled.
Sort All Programs Menu by Name	The Sort All Programs Menu by Name option can be enabled or disabled.
System Administrative Tools	The System Administrative Tools icon can be configured to be displayed on the All Programs menu, on the All Programs menu and the Start Menu, or not displayed at all.
Use Large Icons	The Use Large Icons option can be enabled or disabled.
Start Menu Size	Configures the number of recent programs to display.
Internet Link	Configures whether an Internet link will appear on the Start Menu, and allows you to select the web browser to display.
E-mail Link	Configures whether an e-mail program will be displayed on the Start Menu, and allows you to select which mail program to display.

Configuring Notification Area Properties

The Notification Area tab of the Taskbar and Start Menu Properties dialog box allows you to configure which icons will appear in the notification area, as shown in Figure 4.4. You can configure the Hide Inactive Icons options so that unused icons will be removed from the notification area. You can also configure which system icons will be displayed, including the Clock, Volume, Network, and Power icons.

Configuring Toolbar Options

The Toolbar tab of Taskbar and Start Menu Properties dialog box allows you to configure which toolbars will be displayed on the taskbar, as shown in Figure 4.5. The toolbars that can be displayed include the Address, Windows Media Player, Links, Tablet PC Input Panel, Desktop, and Quick Launch toolbars. The Quick Launch toolbar is enabled by default, and the other toolbars are disabled by default.

FIGURE 4.4 Notification Area tab of the Taskbar and Start Menu Properties dialog box

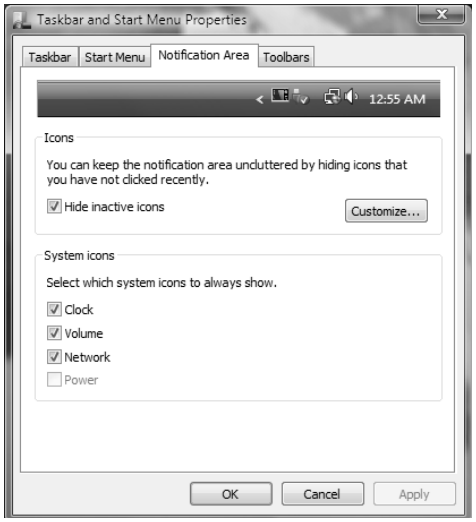
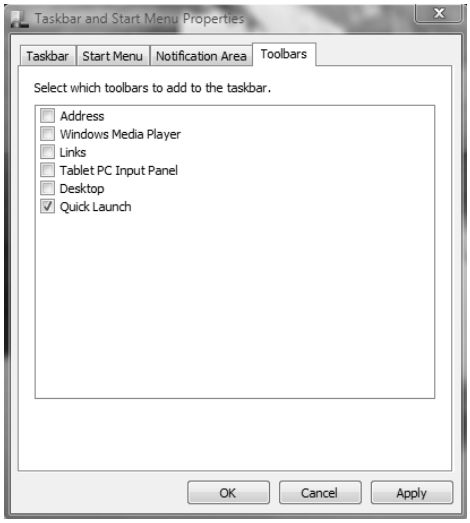


FIGURE 4.5 Toolbars tab of the Taskbar and Start Menu Properties dialog box



In Exercise 4.1, you will check your current taskbar and Start Menu configuration and then configure taskbar and Start Menu properties.

EXERCISE 4.1

Configuring Taskbar and Start Menu Options

1. Select Start ➢ All Programs. Note the size of the icons in the Start Menu. Notice that there is no Programs menu item for Administrative Tools.
2. Right-click an empty space on the taskbar and choose Properties.
3. Click the Start Menu tab. Verify that the Start Menu button is selected, and click the Customize button.
4. In the Customize Start Menu dialog box, scroll down to System Administrative Tools, click Display on the All Programs menu, and then click OK twice.
5. Select Start ➢ All Programs, and note that the All Programs menu lists Administrative Tools.
6. Edit the taskbar and Start Menu properties as you like, or return them to their default settings.

Using Shortcuts

Shortcuts are links to items that are accessible from your computer or network. You can use a shortcut to quickly access a file, program, folder, printer, or computer from your Desktop. Shortcuts can exist in various locations, including on the Desktop, on the Start Menu, and within folders.

To create a shortcut from Windows Explorer, just right-click the item for which you want to create a shortcut, and select Create Shortcut from the context menu. Then you can click the shortcut and drag it to where you want it to appear.

In Exercise 4.2, you will create a shortcut and place it on the Desktop.

EXERCISE 4.2

Creating a Shortcut

1. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer to start Windows Explorer.
2. Expand Computer, then Local Disk, then Windows, and then System32. On the right side of the screen, click Show the Contents of This Folder.
3. On the right side of the screen, scroll down until you see *calc*. Right-click calc, and select Send To ➢ Desktop (create shortcut). A shortcut to `calc.exe` will be placed on the desktop.

Setting Display Properties

The options in the Personalization dialog box, shown in Figure 4.6, allow you to customize the appearance of your Desktop. You can access this dialog box by right-clicking an empty area on the Desktop and selecting Personalize from the context menu. Alternatively, you can select Start ➢ Control Panel ➢ Appearance and Personalization ➢ Personalization.

The Personalization dialog box includes several configurable options that control various aspects of your display:

Windows Color and Appearance This allows you to fine-tune the color and style of your windows.

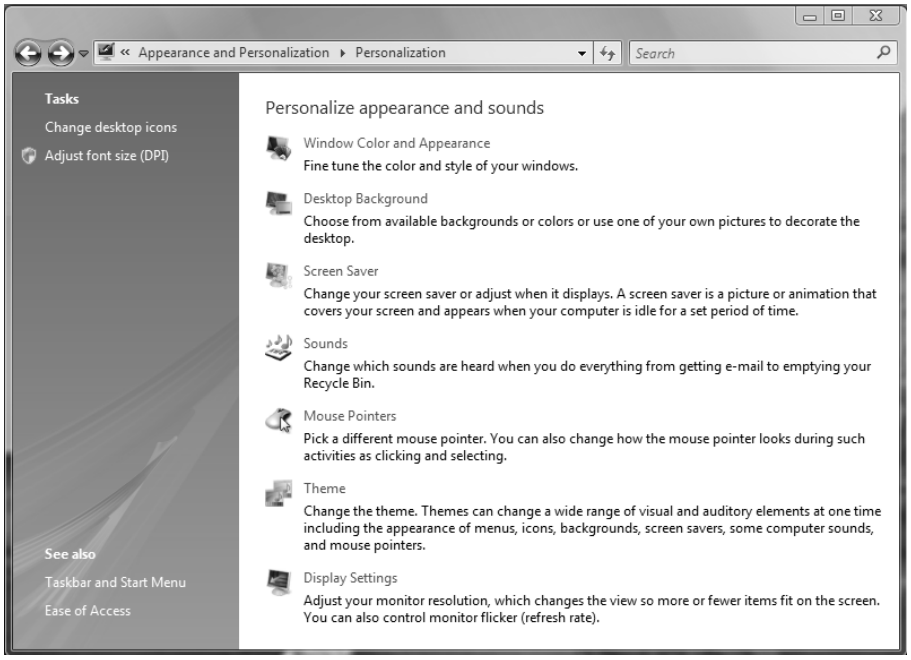
Desktop Background This lets you pick your Desktop background, which uses a picture or an HTML document as wallpaper.

Screen Saver This lets you select a screen saver that will start after the system has been idle for a specified amount of time. You can also specify a password that must be used to re-access the system after it has been idle. When the idle time has been reached, the computer will be locked, and the password of the user who is currently logged on must be entered to access the computer. You can also adjust monitor power settings.

Sounds This lets you choose the sounds that will be played based on the action taken.

Mouse Pointers This allows you to customize the appearance of the mouse pointers.

FIGURE 4.6 The Personalization dialog box



Theme This allows you to select the desktop theme to use. Changing the theme modifies many aspects of the desktop environment, including the appearance of menus, icons, background, screen savers, sounds, and mouse pointers.

Display settings This lets you modify the screen resolution and refresh rate.

Configuring the display is covered in detail in Chapter 3, "Configuring the Windows Vista Environment."

In Exercise 4.3, you will configure display options.

EXERCISE 4.3

Configuring Display Options

1. Right-click an unoccupied area on the Desktop, and select Personalize to open the Personalization dialog box.
2. Select Desktop Background, and then select the picture to use as the desktop background. Configure the picture to be stretched across the screen by selecting the first option in the How Should the Picture Be Positioned? area. Click OK.
3. Click Screen Saver, select the Aurora screen saver, and specify a wait of five minutes. Click OK.
4. Click the Window Color and Appearance option, and then select the Graphite option. Click OK.
5. Change the display settings to suit your personal preferences, and then close the Personalization dialog box.

Configuring Personal Preferences

The most common configuration change made by users is to configure their Desktop. This lets them use the computer more efficiently, and the customization makes them more comfortable with it.

To help users work more efficiently with their computers, you should determine which applications or files are frequently and commonly used and verify that shortcuts or Start Menu items are added for those elements. You can also remove shortcuts or Start Menu items for elements that are used seldom or not at all, helping to make the work area less cluttered and confusing.

Less-experienced users will feel more comfortable with their computer if they have a Desktop personalized to their preferences. This might include their choice of Desktop theme (for example, Windows Vista Aero or Windows Classic themes) and screen saver.

All the exercises in this book assume you are using the Windows Vista Aero theme.

Through the Mouse and Keyboard icons in Control Panel, you can specify your personal preferences for mouse and keyboard settings. We cover mouse and keyboard properties in Chapter 3.

Configuring Windows Sidebar

Windows Sidebar is a new feature of Windows Vista that can be displayed on the side of your desktop. Windows Sidebar holds other programs, called gadgets, that provide quick, visual representations of information, such as the weather, RSS feeds, your calendar, and the current time. Windows Sidebar is easy to customize by adding and removing gadgets.

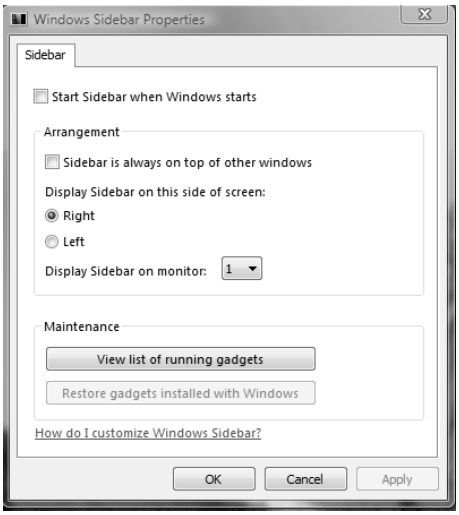
Windows Sidebar is installed by default on Windows Vista. To enable Windows Sidebar, you can click Start ➢ Computer ➢ C: ➢ Program Files ➢ Windows Sidebar ➢ sidebar.exe. Once enabled, Windows Sidebar is displayed as shown in Figure 4.7.

FIGURE 4.7 Windows Sidebar

You can configure options for Windows Sidebar, such as on which side of the screen the Sidebar should appear, whether the Sidebar is always displayed on top of other windows, and whether to start Windows Sidebar when Windows starts. These options can be configured on the Windows Sidebar Properties dialog box, shown in Figure 4.8. To open the Windows Sidebar Properties dialog box, click Start ➢ Control Panel ➢ Appearance and Personalization ➢ Windows Sidebar Properties.

In Exercise 4.4, you'll configure options for Windows Sidebar.

FIGURE 4.8 The Windows Sidebar Properties dialog box



EXERCISE 4.4

Configuring Windows Sidebar Options

1. Open the Windows Sidebar Properties dialog box by clicking Start ➢ Control Panel ➢ Appearance and Personalization ➢ Windows Sidebar Properties.
2. Select the Start Sidebar when Windows Starts option.
3. Select the Sidebar Is Always on Top of Other Windows option.
4. Configure the Sidebar to be displayed on the right side of the screen by selecting the Right option.
5. Click OK.

Managing Multiple Languages and Regional Settings

In addition to configuring your Desktop, you can configure the language and regional settings that are used on your computer Desktop. Windows Vista supports multiple languages through the use of multilanguage technology. Multilanguage technology is designed to meet the following needs:

- Provide support for multilingual editing of documents
- Provide support for various language interfaces in your environment
- Allow users who speak various languages to share the same computer

In the following sections, you will learn about multilingual technology, what options are available for Windows Vista multilingual support, and how to enable and configure multilingual support.

Using Multilingual Technology

Windows Vista is built upon Multilanguage User Interface (MUI) technology and, thus, supports user options to view, edit, and process documents in a variety of languages. These options are provided through Unicode support, National Language Support API, Multilingual API, language files, and Multilingual developer support. Each is discussed here:

Unicode This is an international standard that allows character support for the common characters used in the world's most common languages.

National Language Support API This is used to provide information for locale, character mapping, and keyboard layout. *Locale settings* are used to set local information such as date and time format, currency format, and country names. Character mapping arranges the mapping of local character encodings to Unicode. Keyboard layout settings include character typing information and sorting information.

Multilingual API This is used to set up applications to support keyboard input and fonts from various language versions of applications. For example, Japanese users will see vertical text, and Arabic users will see right-to-left ligatures. This technology allows users to create mixed-language documents.

Language files These are files in which Windows Vista stores all language-specific information, such as text for help files and dialog boxes. They are separate from the operating system files. System code can thus be shared by all language versions of Windows Vista, which allows modular support for different languages.

Multilingual developer support This is a special set of APIs that enables developers to create generic code and then provide support for multiple languages.

Configuring Windows Vista Multilanguage Support

Multilanguage support is implemented using Multilanguage User Interfaces (MUI) technology, which allows the Windows Vista user interface to be presented in different languages and for applications to be viewed and edited in different languages based on the language file selected.

Depending on the level of language support required by your environment, you may use either a localized version of Window Windows Vista or install language files to support multiple languages. The following sections describe these versions and how to configure multilanguage support.

Using Localized Versions of Windows Vista

Microsoft provides localized editions of Windows Vista. For example, users in the United States will most likely use the English version, and users in Japan will most likely use the Japanese version. Localized versions of Windows Vista include fully localized user interfaces for the language that was selected. In addition, localized versions allow users to view, edit, and print documents in many different languages.

Using Windows Vista Language Packs

Windows Vista MUI support provides user interfaces in several languages. This is useful in multinational corporations where users speak several languages and must share computers. It is also appropriate when administrators want to deploy a single image of Windows Vista worldwide. You can manage multiple users who share a single computer and speak different languages through user profiles (covered in Chapter 5, "Configuring Users and Groups") or through group policies (covered in Chapter 6, "Configuring Security").

To implement multilanguage support, the appropriate language files to be implemented must be installed on the computer. There are two types of languages files in Windows Vista:

Multilingual User Interface Pack (MUI) This type of language file provides a translated version of the majority of the user interface. A license is required to use MUIs.

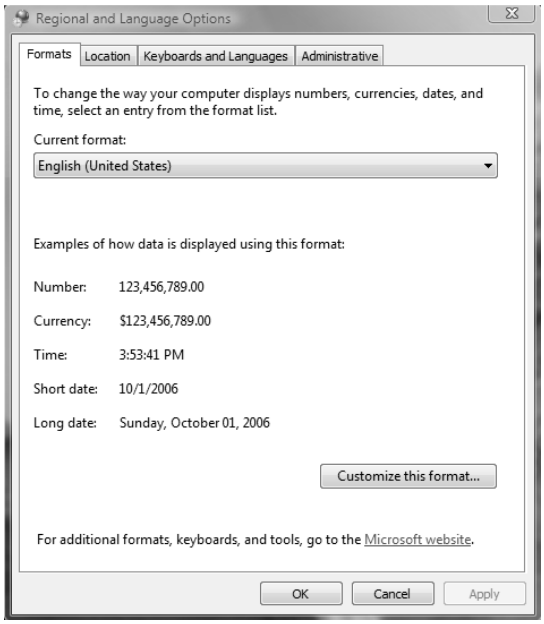
Language Interface Pack (LIP) LIP language files consist of freely available files that provide a translated version of the most popular aspects of the user interface. LIPs require a parent language because LIP files do not translate all components of the user interface.

Enabling and Configuring Multilingual Support

On Windows Vista, you enable and configure multilingual editing and viewing through Start ➢ Control Panel ➢ Clock, Language and Region ➢ Regional and Language Options. This allows access to the Regional and Language Options dialog box, shown in Figure 4.9.

Through Regional and Language Options you can configure Formats, Location, Keyboards and Languages, and Administrative settings. We will look at each of these in the following sections.

FIGURE 4.9 The Regional and Language Options dialog box



Configuring Format Options

The Formats tab of the Regional and Language Options dialog box enables you to configure how numbers, currencies, dates, and times are displayed on the screen. You can change the current format using the Current Format drop-down list, which provides many different format options such as English (United States), German (Germany), and Chinese (Singapore). The Customize This Format button provides the ability to customize how numbers, currencies, times, and dates are displayed based on user or corporate preferences.

Configuring Location Options

The Location tab of the Regional and Language Options dialog box enables you to specify the current location to use in software that provides localized information, such as news and weather information. The Current Location drop-down list provides you with a list of locations that can be selected.

Configuring Keyboard and Language Options

The Keyboards and Languages tab of the Regional and Language Options dialog box enables you to configure the input and keyboard language, and enables you to install or uninstall language

packs. This tab also provides the ability to configure the language bar options and advanced keyboard settings. Clicking the Install/Uninstall Languages button opens the Install or Uninstall Display Languages wizard, which allows you to select the languages to install or uninstall on your computer.

Configuring Administrative Options

The Administrative tab allows you to support languages for non-Unicode programs. This enables non-Unicode programs to display menus and dialog boxes in the user's native language. This tab also allows you to copy the current settings to reserved accounts, such as the default user account or to system accounts.

In Exercise 4.5, you will configure the locale settings on your computer.

EXERCISE 4.5

Configuring Locale Settings

1. Select Start ➢ Control Panel ➢ Clock, Language and Region ➢ Regional and Language Options.
2. One by one, click the Formats, Location, Keyboards and Languages, and Administrative tabs and note the configurations on each tab.
3. Click the Formats tab, and select the Danish (Denmark) option from the Current Format drop-down list. Then click the Apply button.
4. In the Number, Currency, Time, and Date fields, note the changed configurations.
5. Reset your locale to the original configuration, and click Apply.

Real World Scenario

Supporting Multilingual Environments

Your company has an office in Tokyo. Computers are shared by users there who require both English and Japanese language support, for document management as well as the UI. Your CIO has asked you to set up a system that lets users in the Tokyo office use Windows Vista in any language.

To do this, you must install each language file to use. Each computer user can select the preferred UI and specify locale information. This is stored as part of the user's profile. When you log on as a specific user, you see the linguistic and locale information that has been configured.

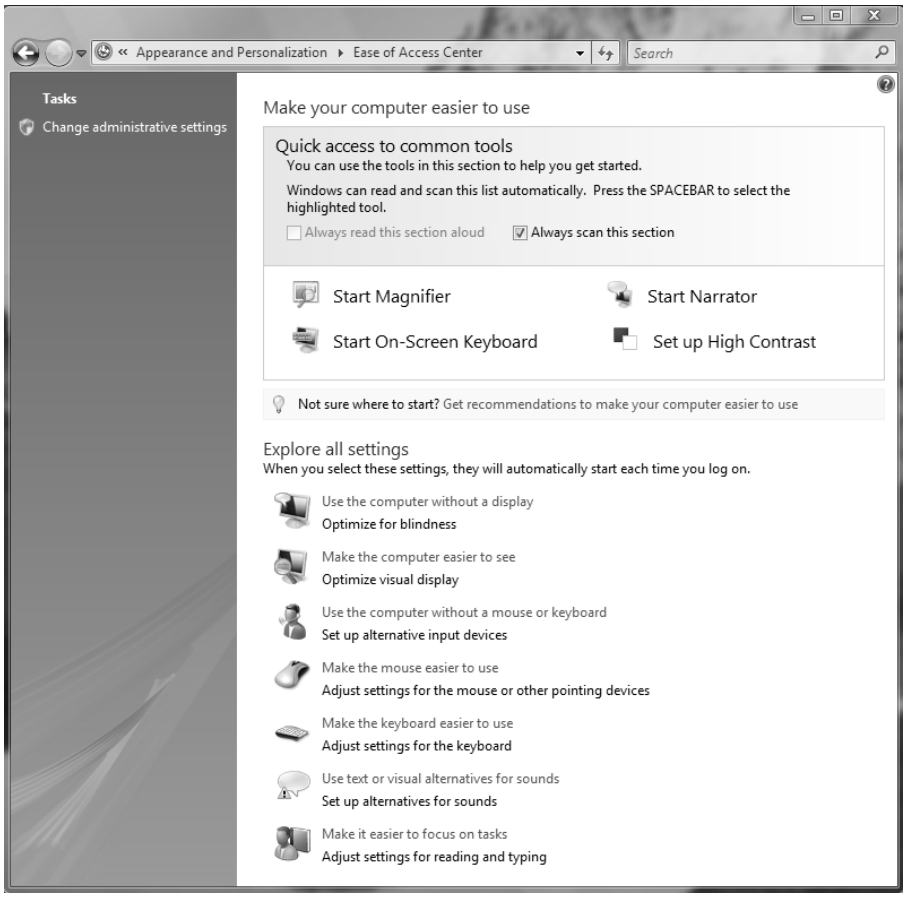
Configuring Accessibility Features

Windows Vista allows you to configure the Desktop so those users with special accessibility needs can use the Windows Vista Desktop more easily. Through its accessibility options and accessibility utilities, Windows Vista supports users with limited sight, hearing, or mobility. The following sections describe how to use these accessibility features.

Setting Accessibility Options

Through the Ease of Access Center available in Control Panel, you can configure keyboard, sound, display, mouse, and general properties of Windows Vista for users with special needs. To access the Accessibility Options dialog box (see Figure 4.10), select Control Panel ➢ Appearance and Personalization, and then click Ease of Access Center.

FIGURE 4.10 The Ease of Access Center dialog box



The Ease of Access Center provides several options for customizing the computer to make it easier to use. Some commonly configured accessibility options include magnifying the text on the screen, configuring the text on the screen to be narrated, configuring an on-screen keyboard, and configuring a high-contrast desktop environment. Here are some other settings that can be modified for improved accessibility:

Use the Computer Without a Display This configures the computer to be optimized for visually impaired users. You can turn on the narrator, turn on audio descriptions, and turn off animations.

Make the Computer Easier to See This option configures the display to be optimized for users with sight impairments. You can select a high-contrast color scheme, turn on the narrator and audio descriptions, turn on the screen magnifier, and fine-tune display effects.

Use the Computer Without a Mouse or Keyboard This option configures the computer to use an alternative input device. You can configure the on-screen keyboard to be displayed, or you can configure speech recognition.

Make the Mouse Easier to Use This option adjusts the appearance of the mouse pointer, whether the keyboard should be used to move the mouse around, and whether hovering over a window will activate the window.

Make the Keyboard Easier to Use This option optimizes the keyboard configuration. This contains settings for using Sticky Keys, Filter Keys, and Toggle Keys. Sticky Keys allows the Shift, Ctrl, Alt, or Windows key to be used in conjunction with another key by pressing the keys separately rather than simultaneously. Filter Keys ignores brief or repeated keystrokes and slows the repeat rate. Toggle Keys makes a noise whenever you press the Caps Lock, Num Lock, or Scroll Lock key.

Use Text of Visual Alternatives for Sounds This allows you to specify whether you want to use Sound Sentry, which generates a visual warning whenever the computer makes a sound, and whether to display captions for speech and sounds on your computer.

Make It Easier to Focus on Tasks This allows you to configure settings for optimizing reading and typing settings, and animations.

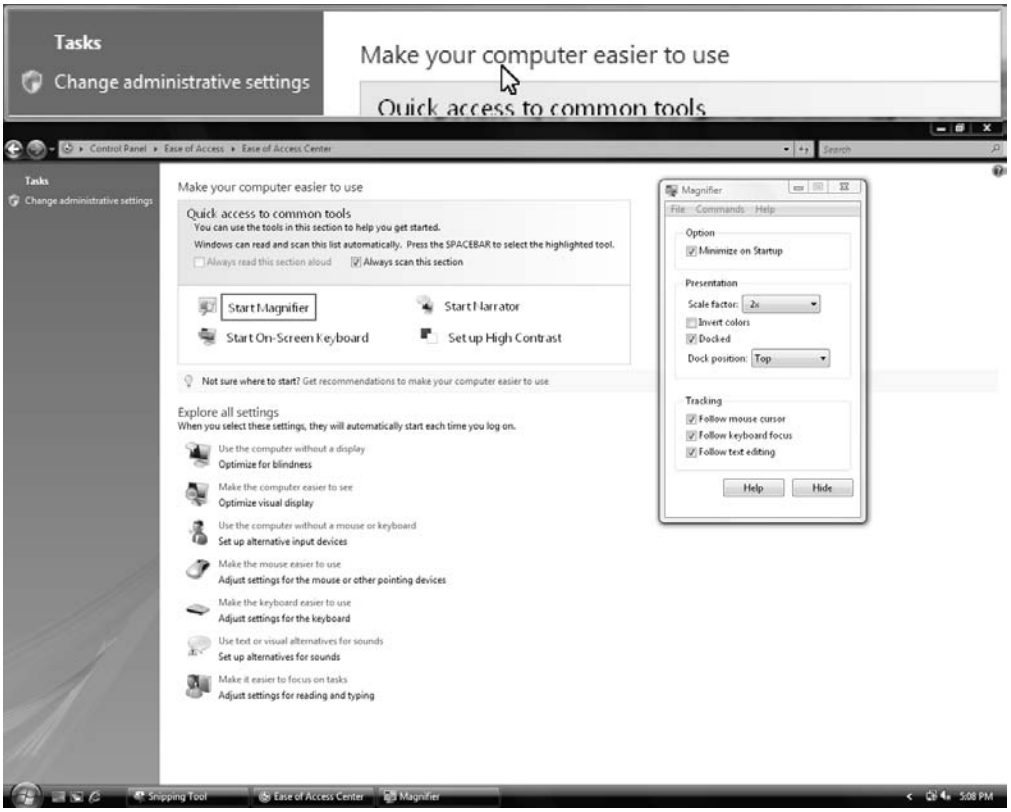
Using Accessibility Utilities

Windows Vista provides several accessibility utilities, including the Magnifier, Narrator, and the On-Screen Keyboard. We cover each of these options in more detail in the following sections.

Using the Magnifier Utility

The *Magnifier utility* creates a separate window to magnify a portion of your screen, as shown in Figure 4.11. This option is useful for users who have poor vision. To access Magnifier, select Start ➢ All Programs ➢ Accessories ➢ Ease of Access ➢ Magnifier.

FIGURE 4.11 The Magnifier utility



Using the Narrator Utility

The *Narrator utility* can read aloud on-screen text, dialog boxes, menus, and buttons. This utility requires that you have some type of sound output device installed and configured. To access Narrator, select Start ➢ All Programs ➢ Accessories ➢ Accessibility ➢ Narrator. This brings up the dialog box shown in Figure 4.12.

Using the On-Screen Keyboard

The *On-Screen Keyboard* displays a keyboard on the screen, as shown in Figure 4.13. Users can use the On-Screen Keyboard keys through a mouse or another input device as an alternative to the keys on the regular keyboard. To access the On-Screen Keyboard, select Start ➢ All Programs ➢ Accessories ➢ Accessibility ➢ On-Screen Keyboard.

FIGURE 4.12 The Microsoft Narrator dialog box

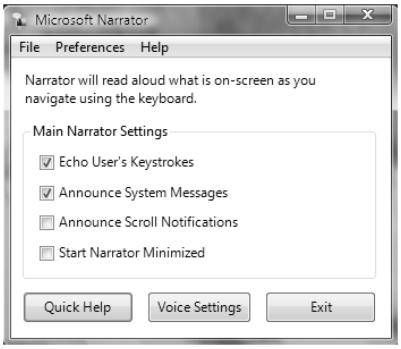


FIGURE 4.13 The On-Screen Keyboard

In Exercise 4.6, you will use the Windows Vista accessibility features.

EXERCISE 4.6

Using Accessibility Features

1. Select Start ➢ All Programs ➢ Accessories ➢ Ease of Access ➢ Magnifier.
2. Experiment with the Magnifier utility. When you have finished, click the Exit button in the Magnifier Settings dialog box.
3. Select Start ➢ All Programs ➢ Accessories ➢ Ease of Access ➢ On-Screen Keyboard.
4. Select Start ➢ All Programs ➢ Accessories ➢ Notepad to open Notepad.
5. Create a text document using the On-Screen Keyboard. When you have finished, close the Notepad document without saving it.
6. Close the On-Screen Keyboard.

Summary

In this chapter, you learned about managing the Windows Vista Desktop. We covered these topics:

- Managing Desktop settings, which include customizing the taskbar and Start Menu, using shortcuts, setting display properties, and configuring Windows Sidebar
- Managing multiple languages and regional settings, which includes configuring multilingual support and choosing locale settings
- Configuring accessibility options and using accessibility utilities

Exam Essentials

Be able to configure Desktop settings. Understand how to customize and configure the Windows Vista Desktop settings, including configuring Windows Sidebar, configuring Windows Aero, creating shortcuts, and configuring the Taskbar and Start Menu.

Know how to configure the computer for multiple-language support. Be able to define the language features that are available in various versions of Windows Vista. Know how to configure locale information and support multiple-language requirements for document processing and the user interface on a single computer.

Be familiar with the accessibility options for users with special needs. Be able to list the accessibility options and their capabilities. Know how to configure the accessibility options.

Review Questions

1. You are the network administrator for a medium-sized company. You support any user Desktop issues. Dan is using Windows Vista on his laptop computer. Programs he frequently uses are not on the taskbar or Start Menu, and programs he has never used are still listed from the manufacturer's initial install. Which of the following options should Dan use to configure the taskbar and Start Menu in Windows Vista?

   A. Right-click an empty space on the taskbar and choose Properties from the context menu.

   B. Select Control Panel ➢ Menu Settings.

   C. Right-click My Computer and choose Manage from the context menu.

   D. Right-click My Computer and choose Properties from the context menu.

2. You are the network administrator for a multinational company. Tran, a user in San Jose, California, is the account manager for all accounts in Vietnam. Tran needs to be able to create and view files in Vietnamese. What support needs to be configured on her computer?

   A. You need to install the appropriate language file to support Vietnamese.

   B. You need to enable supplemental language support to install files for East Asian languages.

   C. You need to install language support for non-Unicode programs.

   D. You need to set Regional Options for Vietnam.

3. You are the network administrator of a large corporation. One of your users, Bob, has impaired vision and is having trouble reading documents on his Windows Vista laptop. Which accessibility utility can Bob use to enlarge a portion of the screen for better visibility?

   A. Enlarger

   B. Expander

   C. Magnifier

   D. Microscope

4. You are supporting Windows Vista computers used by a variety of employees from several countries. When they visit your location, each employee would like their Desktop to appear as it would in their native country. Which of the following locale options can you configure for these users through Windows Vista? (Choose all that apply.)

   A. The format of the date displayed on the computer

   B. The language that is used to display the UI

   C. The currency symbol used by default on the computer

   D. The format of the time displayed on the computer

5. You work on the help desk for a large company. One of your users calls you and reports that they just accidentally deleted their `C:\Documents\Timesheet.xls` file. What is the easiest way to recover this file?

   A. In Folder Options, click the Show Deleted Files option.

   B. In Folder Options, click the Undo Deleted Files option.

   C. Click the Recycle Bin icon on the Desktop and restore the deleted file.

   D. Restore the file from your most recent tape backup.

6. Jeff has a new display adapter and monitor. He wants to set display properties for his Desktop. Which of the following options are NOT set through the Personalization dialog box?

   A. Desktop background

   B. Screen saver

   C. Special visual effects for your Desktop

   D. Contrast and brightness of the monitor

7. You sit in a busy area of the office. Sometimes, you forget to log off or lock the computer when you leave your desk. How can you configure your computer so that it will become password protected if it is idle for more than 10 minutes?

   A. Through the Logon/Logoff icon in Control Panel

   B. Through the Screen Saver option on the Personalization dialog box

   C. Through the Security icon in Control Panel

   D. Through the Security properties of Local Users and Groups

8. Cindy has just installed Windows Vista on her home computer. The Windows Vista version she is using is localized for English. Cindy would also like to be able to use Simplified Chinese to create documents to send to her friends in Taiwan. How can she configure the computer to support Simplified Chinese language settings?

   A. Through Control Panel ➢ Clock, Language and Region ➢ Regional and Language Options ➢ Formats tab

   B. Through Control Panel ➢ Clock, Language and Region ➢ Regional and Language Options ➢ Keyboards and Languages tab

   C. Through Control Panel ➢ Date, Time, Language and Regional Options ➢ Regional and Language Options ➢ Location tab

   D. Only by upgrading to a version of Windows Vista that supports MUI

9. Meredith is a user with limited mobility. She wants to use an alternate method of input instead of a regular keyboard. What options can you configure using Windows Vista? (Select all that apply.)

   A. Configure and install a joystick to use as an input device.

   B. Configure the On-Screen Keyboard to be an input device.

   C. Configure Alternative Serial Devices and install a new serial device.

   D. Configure and install a microphone to use for speech recognition.

10. You administer a network for an office location in Canada. Some of your users have requested that they want to view currency in French instead of English. How can you modify this setting?
    A. Through Control Panel ➢ Clock, Language and Region ➢ Regional and Language Options ➢ Formats tab
    B. Through Control Panel ➢ Clock, Language and Region ➢ Regional and Language Options ➢ Keyboards and Languages tab
    C. Through Control Panel ➢ Date, Time, Language and Regional Options ➢ Regional and Language Options ➢ Location tab
    D. Through Control Panel ➢ Date, Time, Language and Regional Options ➢ Regional and Language Options ➢ Administrative tab

11. Bill is a new employee and you are configuring a Windows Vista computer for him to use. He is visually impaired, and you need to configure the computer so that he can use it. Which of the following options should you configure?
    A. Magnifier
    B. High Contrast
    C. On-Screen Keyboard
    D. Narrator

12. A user in your organization has limited mobility and you want to make it easier for them to perform keyboard actions, particularly for using keyboard shortcuts. Which of the following options should you configure?
    A. Narrator
    B. Sticky Keys
    C. Filter Keys
    D. Toggle Keys

13. You are the network administrator for your organization. You are configuring a computer for Lisa, who has mentioned that she has difficulty using the keyboard and often has to delete repeated keystrokes. She has asked if you can help her reduce the additional work that she is performing because of this. Which of the following options could you configure?
    A. Sticky Keys
    B. Easy Keys
    C. Filter Keys
    D. Toggle Keys

14. You are the network administrator for your organization. You are configuring a Windows Vista computer for one of your users. You want to configure the computer so that a tone is played when the Caps Lock key is pressed. Which of the following options could you configure?
    A. Sticky Keys
    B. Easy Keys
    C. Filter Keys
    D. Toggle Keys

15. You are an administrator for your company's network. You want to configure the volume control and the clock to be displayed on the desktop of your users' computers. How can you accomplish this task?

A. Through Control Panel ➢ Appearance and Personalization ➢ Personalization

B. Through Control Panel ➢ Appearance and Personalization ➢ Taskbar and Start Menu

C. Through Control Panel ➢ Appearance and Personalization ➢ Windows Sidebar Properties

D. Through Control Panel ➢ Appearance and Personalization ➢ Ease of Access Center

16. Several users in your organization need to edit documents in multiple languages. You have installed the necessary languages on each of the users' computers. You want to enable the users to more easily change the language used, and you want to enable this through the use of the Language Bar in the taskbar. How can you enable this option?

A. By right-clicking an empty space of the taskbar, selecting Properties, and clicking the Toolbars tab

B. By clicking Control Panel ➢ Appearance and Personalization ➢ Taskbar and Start Menu and clicking the Toolbars tab

C. By clicking Control Panel ➢ Clock, Language, and Region ➢ Regional and Language Options ➢ Keyboards and Languages tab

D. By right-clicking an empty space of the taskbar, selecting Properties, and clicking the Taskbar tab

17. You are configuring an image of Windows Vista that will be deployed to a new office location for your company. You are configuring the desktop. You want to ensure that the taskbar is viewable even when applications are opened in full-screen mode. You also do not want the taskbar to be moved by the users. How can you configure these options?

A. By right-clicking an empty space of the taskbar, selecting Properties, and clicking the Toolbars tab

B. By right-clicking an empty space of the taskbar, selecting Properties, and clicking the Taskbar tab

C. By right-clicking an empty space of the taskbar, selecting Properties, and clicking the Notification Area tab

D. By right-clicking an empty space of the taskbar, selecting Properties, and clicking the Start Menu tab

18. You are the network administrator for a manufacturing company. You are configuring several Windows Vista computers for a group of newly hired engineers. You want to optimize the new computers so that it uses the new user interface enhancements included with Windows Vista. How can you accomplish this task?

A. By right-clicking an empty space of the desktop, selecting Personalize, and clicking Display Settings

B. By right-clicking an empty space of the desktop, selecting Personalize, and clicking Desktop Background

C. By right-clicking an empty space of the desktop, selecting Personalize, and clicking Screen Saver

D. By right-clicking an empty space of the desktop, selecting Personalize, and clicking Theme

19. You are configuring a computer to be deployed to another network administrator. You want to allow the other administrator to quickly access the Administrative Tools options available with Windows Vista. How can you accomplish this task?

A. By right-clicking an empty space of the taskbar, selecting Properties, and clicking Desktop on the Toolbars tab

B. By right-clicking an empty space of the taskbar, selecting Properties, and clicking Show Quick Launch on the Taskbar tab

C. By right-clicking an empty space of the taskbar, selecting Properties, and clicking Customize on the Start Menu tab

D. By right-clicking an empty space of the taskbar, selecting Properties, and clicking Customize on the Notification Area tab

20. You are configuring Windows Sidebar on your Windows Vista computer. You want to ensure that the Sidebar is displayed every time you reboot the computer. Which of the following should you do to accomplish this goal?

A. Enable the Sidebar by clicking Start ➢ Computer ➢ C: ➢ Program Files ➢ Windows Sidebar ➢ sidebar.exe. The Sidebar will be configured to be displayed every time the computer is rebooted.

B. Install Windows Sidebar by clicking Start ➢ Computer ➢ C: ➢ Program Files ➢ Windows Sidebar ➢ sidebar.exe. The Sidebar will automatically be configured to start every time the computer boots.

C. Open the Windows Sidebar properties dialog box by clicking Start ➢ Control Panel ➢ Appearance and Personalization ➢ Windows Sidebar Properties. Select the Start Sidebar When Windows Starts option.

D. Open the Windows Sidebar properties dialog box by clicking Start ➢ Control Panel ➢ Appearance and Personalization ➢ Windows Sidebar Properties. Configure the Display Sidebar on Monitor option.

Answers to Review Questions

1. A. The easiest way to configure the taskbar and Start Menu properties is by right-clicking an open area of the Taskbar and choosing Properties. There is no Menu Settings option in Control Panel.

2. A. You should install the appropriate language files to support Vietnamese. Additional language files can be installed on a Windows Vista computer to provide multiple-language support.

3. C. The Magnifier utility creates a separate window that magnifies the portion of the screen that is being used. None of the other choices exists in Windows Vista.

4. A, C, D. Locale settings are used to configure regional settings for numbers, currency, time, date, and input locales.

5. C. The easiest way to recover a deleted file is to restore it from the Recycle Bin. The Recycle Bin holds all of the files and folders that have been deleted, as long as there is space on the disk. From this utility, you can retrieve or permanently delete files.

6. D. Through the Personalization dialog box, you can set your Desktop background, the screen saver to be used by your computer, and any special visual effects for your Desktop. Contrast and brightness of the monitor are typically set through the monitor's controls.

7. B. The Screen Saver option of the Personalization dialog box allows you to select a screen saver that will start after the computer has been idle for a specified amount of time. You can configure the screen saver to require the user's password in order to resume the computer's normal function. When the password is invoked, the computer will be locked. To access the locked computer, you must enter the password of the user who is currently logged on or an administrator password.

8. B. To install different language packs, Cindy should enable and configure additional languages by using the Keyboards and Languages tab in the Regional and Language Options dialog box.

9. A, B, D. Windows Vista supports several alternate input options instead of the regular keyboard and mouse pointer. You can configure the On-Screen Keyboard, which will allow Meredith to type using the mouse pointer. You can configure a joystick device as an input device in conjunction with the On-Screen Keyboard instead of the regular keyboard. You can also configure speech recognition so that Meredith can say the commands or text to be inputted into the computer.

10. A. You can modify format settings such as numbers, currencies, dates, and times using the Formats tab of the Regional and Language Options dialog box. Windows Vista supports many different format options for these settings. Additionally, you can customize the standard format options for a specific setting.

11. D. You should configure the Narrator so that it starts each time the computer is booted. The Narrator reads aloud the text on the screen, so visually impaired users can utilize the computer.

12. B. You should configure Sticky Keys so that keyboard shortcuts can be pressed one key at a time instead of simultaneously. Sticky Keys, Toggle Keys, and Filter Keys are settings that can be configured to make it easier to type using the keyboard.

13. C. You should configure Filter Keys so that repeated keystrokes are ignored. Filter Keys also allows you to adjust the keyboard repeat rates. Sticky Keys, Toggle Keys, and Filter Keys are settings that can be configured to make it easier to type using the keyboard. Easy Keys is not an option for making the keyboard easier to use.

14. D. You should configure Toggle Keys so that a tone is played when the Caps Lock, Num Lock and Scroll Lock key is pressed. Toggle Keys can be enabled by pressing the Num Lock key and holding it down for five seconds. Sticky Keys, Toggle Keys, and Filter Keys are settings that can be configured to make it easier to type using the keyboard.

15. B. You can configure notification area options, such as displaying the clock and volume icon, through Control Panel ➢ Appearance and Personalization ➢ Taskbar and Start Menu and then clicking the Notification Area tab. The Network icon can also be displayed on the Desktop by using this tab. You can also reach this tab by right-clicking an empty area of the taskbar and selecting Properties from the context menu.

16. C. You can configure the Language Bar by clicking Control Panel ➢ Clock, Language, and Region ➢ Regional and Language Options ➢ Keyboards and Languages tab. Then, you can click the Change Keyboards button, which opens the Text Services and Input Languages dialog box. Click the Language Bar tab on this dialog box to enable and configure the Language Bar. The Language Bar provides quick access to language options from the taskbar.

17. B. You can configure taskbar options by right-clicking an empty space of the taskbar, selecting Properties, and clicking the Taskbar tab. This tab contains several options for configuring the taskbar, such as Lock the Taskbar, Auto-Hide the Taskbar, Keep the Taskbar on Top of Other Windows, Group Similar Taskbar Options, Show Quick Launch, and Show Window Previews (Thumbnails).

18. D. You can configure user interface settings by clicking an empty space on the Desktop and selecting Personalize. The Theme option of the Personalization dialog box allows you to select from a number of themes available with Windows Vista. The Windows Vista Aero theme includes new user interface elements, such as transparent windows and new color schemes. Other theme options with Windows Vista include Windows Vista Basic, Windows Vista Standard, and Windows Classic.

19. C. You can configure Start Menu options by clicking an empty space of the taskbar, selecting Properties, and clicking Customize on the Start Menu tab, which opens the Customize Start Menu dialog box. This dialog box provides a list of configuration options that customize how items are displayed on the Start Menu. The System Administrative Tools option configures how the Administrative Tools icon is displayed. You can configure the Administrative Tools icon to be displayed on the All Programs menu, to be displayed on both the All Programs menu and the Start Menu, or not to be displayed on either the Start Menu or the All Programs menu.

20. C. You can configure Windows Sidebar to start every time Windows starts by selecting the Start Sidebar When Windows Starts option found on the Windows Sidebar Properties dialog box. The Windows Sidebar Properties dialog box can be access by clicking Start ➢ Control Panel ➢ Appearance and Personalization ➢ Windows Sidebar Properties. The Display Sidebar on Monitor option allows you to configure where the Sidebar will be displayed in a multiple-monitor setup.

Chapter

5

Configuring Users and Groups

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring and Troubleshooting Post-Installation System Settings**
  - Troubleshoot post-installation configuration issues
- ✓ **Configuring Windows Security Features**
  - Configure and troubleshoot User Account Control

One of the most fundamental tasks in network management is creating user and group accounts. Without a *user account*, a user cannot log on to a computer, server, or network.

When users log on, they supply a username and password. Then their user accounts are validated by a security mechanism. In Windows Vista, users can log on to a computer locally, or they can log on through Active Directory.

When you first create users, you assign them usernames, passwords, and password settings. After a user is created, you can change these settings and select other options for that user through the User Accounts Control Panel.

Group accounts are used to ease network administration by grouping users who have similar permission requirements together. Groups are an important part of network management. Many administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users. Windows Vista includes built-in local groups, such as Administrators and Backup Operators. These groups already have all the permissions needed to accomplish specific tasks. Windows Vista also uses default special groups, which are managed by the system. Users become members of special groups based on their requirements for computer and network access.

You create and manage local groups through the Local Users and Groups utility. With this utility, you can add groups, change group membership, rename groups, and delete groups.

In this chapter, you will learn about user management at the local level, including creating user accounts and managing user properties. Then you will learn how to create and manage local groups.

Overview of Windows Vista User Accounts

When you install Windows Vista, several user accounts are created automatically. You can then create new user accounts. On Windows Vista computers, you can create local user accounts. If your network has a Windows Server 2003 or Windows 2000 Server domain controller, your network can have domain user accounts, as well.

One of the new features included with Windows Vista is *User Account Control*. User Account Control provides an additional level of security by limiting the level of access that

users have when performing normal, everyday tasks. When needed, users can gain elevated access for specific administrative tasks.

In the following sections, you will learn about the default user accounts that are created by Windows Vista and the difference between local and domain user accounts.

Account Types

Windows Vista supports two types of user accounts:

Administrator The Administrator account type provides unrestricted access to performing administrative tasks. As a result, Administrator accounts should be used only for performing administrative tasks and should not be used for normal computing tasks.

Standard User The Standard User type is the account type that should be applied for every user of the computer. Standard User accounts can perform most day-to-day tasks, such as running Microsoft Word, accessing e-mail, using Internet Explorer, and so on. Running as a Standard User increases security by limiting the possibility of a virus or other malicious code from infecting the computer and making systemwide changes, because Standard User accounts are unable to make systemwide changes.

Built-in Accounts

By default, a computer that is installed with Windows Vista in a workgroup has three user accounts:

Administrator The *Administrator account* is a special account that has full control over the computer. The Administrator account can perform all tasks, such as creating users and groups, managing the file system, and setting up printing. Note that the Administrator account is disabled by default.

Guest The *Guest account* allows users to access the computer even if they do not have a unique username and password. Because of the inherent security risks associated with this type of user, the Guest account is disabled by default. When this account is enabled, it is usually given very limited privileges.

Initial user The *initial user* account uses the name of the registered user. By default, the initial user is a member of the Administrators group.

By default, the name Administrator is given to a user account that is a member of the Administrators group. However, in Windows Vista, this user account is disabled by default. You can increase the computer's security by leaving this account disabled, and assigning other members to the Administrators group. This way, a malicious user will be unable to log on to the computer using the Administrator user account.

Local and Domain User Accounts

Windows Vista supports two kinds of users: local users and domain users. A computer that is running Windows Vista has the ability to store its own user accounts database. The users stored at the local computer are known as *local user accounts*.

Active Directory is a directory service that is available with the Windows Server 2003 and Windows 2000 Server platforms. It stores information in a central database that allows users to have a single user account for the network. The users stored in Active Directory's central database are called *domain user accounts*.

If you use local user accounts, they must be configured on each computer that the user needs access to within the network. For this reason, domain user accounts are commonly used to manage users on large networks.

On Windows Vista computers and Windows Server 2003 and Windows 2000 Server member servers (a member server has a local accounts database and does not store Active Directory), you can create local users through the Local Users and Groups utility, as described in the "Working with User Accounts" section later in this chapter. On Windows Server 2003 and Windows 2000 Server domain controllers, you manage users with the Microsoft Active Directory Users and Computers utility.

Active Directory is covered in detail in *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide, 2nd Edition,* by Robert Shimonski and Anil Desai with James Chellis (Sybex, 2006).

Logging On and Logging Off

Users must log on to a Windows Vista computer before they can use that computer. When you create user accounts, you set up the computer to accept the logon information provided by the user. You can log on locally to a Windows Vista computer, or you can log on to a domain. When you install the computer, you specify that it will be a part of a workgroup, which implies a local logon, or that the computer will be a part of a domain, which implies a domain logon.

When users are ready to stop working on a Windows Vista computer, they should log off. Users can log off through the Windows Security dialog box.

In the following sections, you will learn about local user authentication and how a user logs out of a Windows Vista computer.

Using Local User Logon Authentication

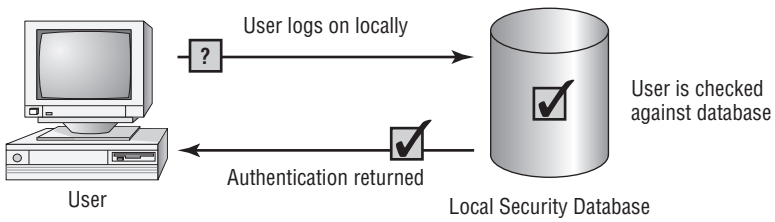
Depending on whether you are logging on to a computer locally or are logging into a domain, Windows Vista uses two different logon procedures. When you log on to a Windows Vista

computer locally, you must present a valid username and password (ones that exist within the local accounts database). As part of a successful *authentication*, the following steps take place:

1. At system startup, the user is prompted to click their username from a list of users who have been created locally. This is significantly different from the Ctrl+Alt+Del logon sequence that was used by Windows NT and Windows 2000. The Ctrl+Alt+Del sequence is still used when you log on to a domain environment. You can also configure this logon sequence as an option in a local environment.
2. The local computer compares the user's logon credentials with the information in the local security database.
3. If the information presented matches the account database, an *access token* is created. Access tokens are used to identify the user and the groups of which that user is a member.

Figure 5.1 illustrates the three main steps in the logon process.

FIGURE 5.1 The logon process



Access tokens are created only when you log on. If you change group memberships, you need to log off and log on again to update the access token.

Other actions that take place as part of the logon process include the following:

- The system reads the part of the Registry that contains user configuration information.
- The user's profile is loaded. (User profiles are discussed in the "Setting Up User Profiles, Logon Scripts, and Home Folders" section later in this chapter.)
- Any policies that have been assigned to the user through a user or group policy are enforced. (Policies for users are discussed later in Chapter 6, "Configuring Security.")
- Any logon scripts that have been assigned are executed. (We discuss assigning logon scripts to users in the "Setting Up User Profiles, Logon Scripts, and Home Folders" section.)
- Persistent network and printer connections are restored. (We discuss network connections in Chapter 8, "Configuring Network Connectivity."

Through the logon process, you can control what resources a user can access by assigning permissions. Permissions are granted to either users or groups. Permissions also determine what actions a user can perform on a computer. In Chapter 6, you will learn more about assigning resource permissions.

Logging Off Windows Vista

To log off Windows Vista, you click Start, point to the arrow next to the Lock button, and then click Logoff. Pressing Ctrl+Alt+Del will also present you with a screen that will allow you to select whether to lock the computer, switch user, log off, change the password, or start Task Manager.

Working with User Accounts

To set up and manage users, you use the *Local Users and Groups* utility or the User Accounts and Family Safety option in the Control Panel. With either option, you can create, disable, delete, and rename user accounts, as well as change user passwords.

Using the Local Users and Groups Utility

There are two common methods for accessing the Local Users and Groups utility:

- You can load Local Users and Groups as a Microsoft Management Console (MMC) snap-in. (See Chapter 3, "Configuring the Windows Vista Environment," for details on the MMC and the purpose of snap-ins.)
- You can access the Local Users and Groups utility through the Computer Management utility.

In Exercise 5.1, you will use both methods for accessing the Local Users and Groups utility.

EXERCISE 5.1

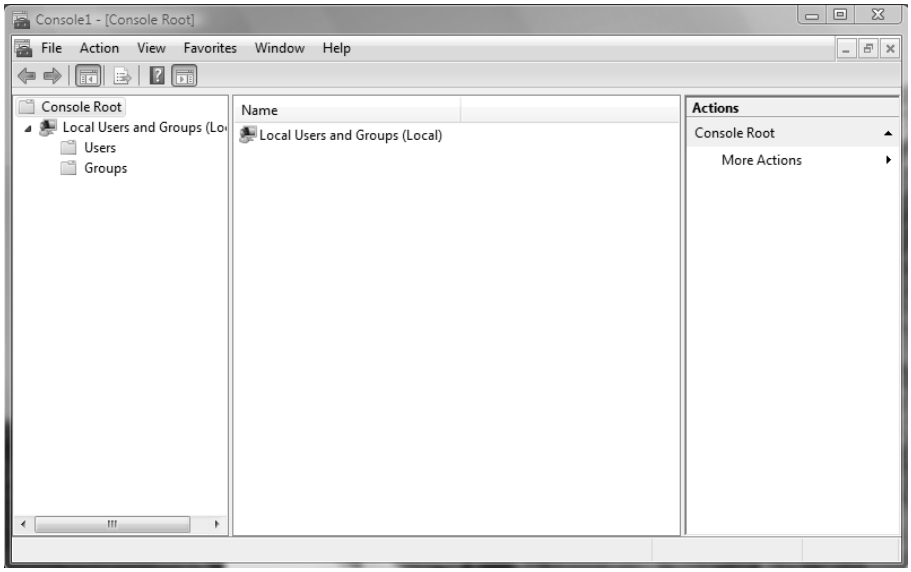
Accessing the Local Users and Groups Utility

In this exercise, you will first add the Local Users and Groups snap-in to the MMC. Next, you will add a shortcut to your Desktop that will take you to the MMC. Finally, you will use the other access technique of opening the Local Users and Groups utility from the Computer Management utility.

EXERCISE 5.1 *(continued)*

Adding the Local Users and Groups Snap-in to the MMC

1. Select Start and in the Search box, type **MMC**, and press Enter.
2. Select File ➢ Add/Remove Snap-in.
3. In the Add/Remove Snap-in dialog box, click the Add button.
4. In the Add Standalone Snap-in dialog box, select Local Users and Groups and click Add.
5. In the Choose Target Machine dialog box, click the Finish button to accept the default selection of Local Computer.
6. Click OK in the Add or Remove Snap-in dialog box.
7. In the MMC window, expand the `Local Users and Groups` folder to see the `Users` and `Groups` folders.



Adding the MMC to Your Desktop

1. Select File ➢ Save. Click the folder with the Up arrow icon until you are at the root of the computer.
2. Select the Desktop option and specify **`Admin Console`** as the filename. The default extension is `.msc`. Click the Save button.

EXERCISE 5.1 *(continued)*

Accessing Local Users and Groups through Computer Management

1. Select Start, and then right-click My Computer and select Manage.
2. In the Computer Management window, expand the `System Tools` folder and then the `Local Users and Groups` folder.

If your computer doesn't have the MMC configured, the quickest way to access the Local Users and Groups utility is through the Computer Management utility.

Using the User Accounts and Family Safety Control Panel Option

The User Accounts and Family Safety Control Panel option provides the ability to manage user accounts, in addition to configuring parental controls and Windows CardSpace information. To access the User Accounts and Family Safety Control Panel option, click Start ➢ Control Panel ➢ User Accounts and Family Safety. Then click the User Accounts option to manage and configure your user accounts on the Windows Vista computer, or click Add or Remove User Accounts to add or remove user accounts on the computer. Figure 5.2 displays the User Accounts and Family Safety dialog box.

Creating New Users

To create users on a Windows Vista computer, you must be logged on as a user with permissions to create a new user, or you must be a member of the Administrators group. In the following sections, you will learn about username rules and conventions, usernames, and security identifiers in more detail.

Username Rules and Conventions

The only real requirement for creating a new user is that you must provide a valid username. "Valid" means that the name must follow the Windows Vista rules for usernames. However, it's also a good idea to have your own rules for usernames, which form your naming convention.

The following are the Windows Vista rules for usernames:

- A username must be from 1 to 20 characters.
- The username must be unique to all other user and group names stored on that specified computer.

- The username cannot contain the following characters:

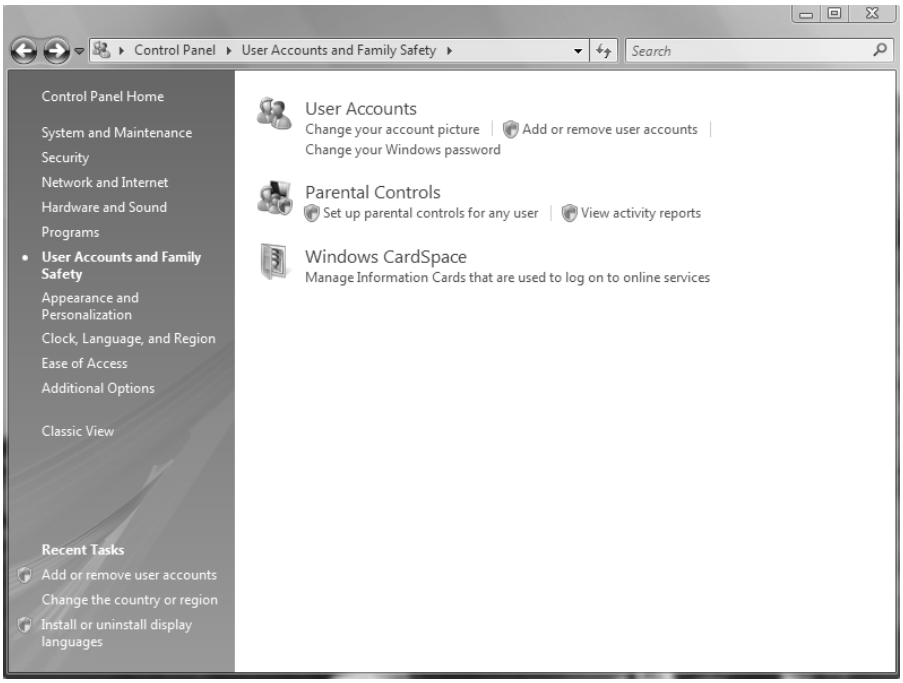
  * / \ [ ] : ; | = , + ? < > “ @

- A username cannot consist exclusively of periods or spaces.

Keeping these rules in mind, you should choose a naming convention (a consistent naming format). For example, consider a user named Kevin Donald. One naming convention might use the last name and first initial, for the username DonaldK. Another naming convention might use the first initial and last name, for the username KDonald. Other user-naming conventions are based on the naming convention defined for e-mail names, so that the logon name and e-mail name match. You should also provide a mechanism that would accommodate duplicate names. For example, if you had a user named Kevin Donald and a user named Kate Donald, you might use a middle initial for usernames, such as KLDonald and KMDonald.

You should also apply naming conventions to objects such as groups, printers, and computers.

FIGURE 5.2 The User Accounts and Family Safety dialog box



Usernames and Security Identifiers

When you create a new user, a *security identifier (SID)* is automatically created on the computer for the user account. The username is a property of the SID. For example, a user SID might look like this:

```
S-1-5-21-823518204-746137067-120266-629-500
```

It's apparent that using SIDs for user identification would make administration a nightmare. Fortunately, for your administrative tasks, you see and use the username instead of the SID.

SIDs have several advantages. Because Windows Vista uses the SID as the user object, you can easily rename a user while still retaining all the properties of that user. SIDs also ensure that if you delete and re-create a user account with the same username, the new user account will not have any of the properties of the old account, because it is based on a new, unique SID. Renaming and deleting user accounts is discussed later in this chapter in the "Renaming User Accounts" and "Deleting User Accounts" sections.

Make sure your users know that usernames are not case sensitive but that passwords are.

In Exercise 5.2, you will use the New User dialog box to create several new local user accounts. We will put these user accounts to work in subsequent exercises in this chapter. Table 5.1 describes all the options available in the New User dialog box.

TABLE 5.1 User Account Options Available in the New User Dialog Box

Option	Description
User Name	Defines the username for the new account. Choose a name that is consistent with your naming convention (e.g., WSmith). This is the only required field. Usernames are not case sensitive.
Full Name	Allows you to provide more detailed name information. This is typically the user's first and last names (e.g., Will Smith). By default, this field contains the same name as the User Name field.
Description	Typically used to specify a title and/or location (e.g., Sales-Nashville) for the account, but it can be used to provide any additional information about the user.

TABLE 5.1 User Account Options Available in the New User Dialog Box *(continued)*

Option	Description
Password	Assigns the initial password for the user. For security purposes, avoid using readily available information about the user. Passwords are case sensitive.
Confirm Password	Confirms that you typed the password the same way two times to verify that you entered the password correctly.
User Must Change Password at Next Logon	If enabled, forces the user to change the password the first time they log on. This is done to increase security. By default, this option is selected.
User Cannot Change Password	If enabled, prevents a user from changing their password. It is useful for accounts such as Guest and accounts that are shared by more than one user. By default, this option is not selected.
Password Never Expires	If enabled, specifies that the password will never expire, even if a password policy has been specified. For example, you might enable this option if this is a service account and you do not want the administrative overhead of managing password changes. By default, this option is not selected.
Account Is Disabled	If enabled, specifies that this account cannot be used for logon purposes. For example, you might select this option for template accounts or if an account is not currently being used. It helps keep inactive accounts from posing security threats. By default, this option is not selected.

Before you start Exercise 5.2, make sure you are logged on as a user with permissions to create new users and have already added the Local Users and Groups snap-in to the MMC (see Exercise 5.1).

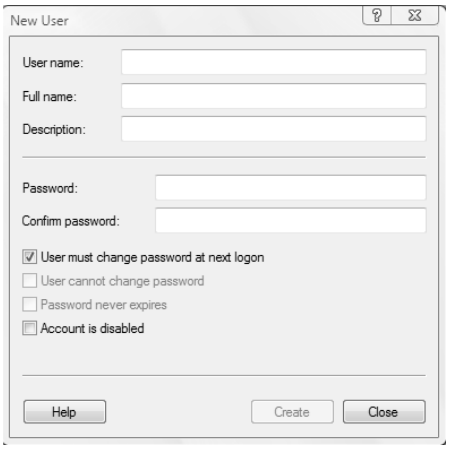
EXERCISE 5.2

Creating New Local Users

1. Open the Admin Console MMC shortcut that was created in Exercise 5.1 and expand the Local Users and Groups snap-in.

EXERCISE 5.2 *(continued)*

2. Highlight the Users folder and select Action ➢ New User. The New User dialog box appears.



3. In the User Name text box, type **Cam**.
4. In the Full Name text box, type **Cam Presely**.
5. In the Description text box, type **Sales Vice President**.
6. Leave the Password and Confirm Password text boxes empty and accept the defaults for the check boxes. Make sure you uncheck the User Must Change Password at Next Logon option. Click the Create button to add the user.
7. Use the New User dialog box to create six more users, filling out the fields as follows:

   Name: **Kevin**; Full Name: **Kevin Jones**; Description: **Sales-Florida**; Password: (blank)

   Name: **Terry**; Full Name: **Terry Belle**; Description: **Marketing**; Password: (blank)

   Name: **Ron**; Full Name: **Ron Klein**; Description: **PR**; Password: **P@ssw0rD**

   Name: **Will**; Full Name: **Will Smith**; Description: **Sales-Nashville**; Password: **v!$t@**

   Name: **Emily**; Full Name: **Emily Buras**; Description: **President**; Password: **P3@ch** (with a capital *P*)

   Name: **Michael**; Full Name: **Michael Phillips**; Description: **Tech Support**; Password: **brainbeacon**

8. After you've finished creating all of the users, click the Close button to exit the New User dialog box.

You can also create users through the command-line utility NET USER. For more information about this command, type `NET USER /?` at a command prompt.

Disabling User Accounts

When a user account is no longer needed, the account should be disabled or deleted. After you've disabled an account, you can later enable it again to restore it with all of its associated user properties. An account that is deleted, however, can never be recovered.

User accounts not in use pose a security threat because an intruder could access your network through an inactive account. User accounts that are no longer needed should be deleted.

You might disable an account because a user will not be using it for a period of time, perhaps because that employee is going on vacation or taking a leave of absence. Another reason to disable an account is that you're planning to put another user in that same function. For example, suppose that Gary, the engineering manager, quits. If you disable his account, when your company hires a new engineering manager, you can simply rename Gary's user account (to the username for the new manager) and enable that account. This ensures that the user who takes over Gary's position will have all the same user properties and own all the same resources.

Disabling accounts also provides a security mechanism for special situations. For example, if your company were laying off a group of people, a security measure would be to disable their accounts at the same time the layoff notices were given out. This prevents those users from inflicting any damage to the company's files after they receive their layoff notice.

In Exercise 5.3, you will disable a user account. Before you follow this exercise, you should have already created new users (see Exercise 5.2).

EXERCISE 5.3

Disabling a User

1. Open the Admin Console MMC shortcut that was created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Open the `Users` folder. Double-click user Kevin to open his Properties dialog box.

EXERCISE 5.3 *(continued)*

3. In the General tab, check the Account Is Disabled box. Click OK.

4. Log off and attempt to log on as Kevin. This should fail, since the account is now disabled.

5. Log back on using your user account.

You can also access a user's Properties dialog box by highlighting the user, right-clicking, and selecting Properties.

Deleting User Accounts

As noted in the preceding section, you should delete a user account if you are sure that the account will never be needed again.

To delete a user, open the Local Users and Groups utility, highlight the user account you wish to delete, and click Action to bring up the menu shown in Figure 5.3. Then select Delete.

Because user deletion is a permanent action, you will see the dialog box shown in Figure 5.4, asking you to confirm that you really wish to delete the account. After you click the Yes button here, you will not be able to re-create or re-access the account (unless you restore your local user accounts database from a backup).

In Exercise 5.4, you will delete a user account. This exercise assumes you have completed the previous exercises in this chapter.

FIGURE 5.3 Deleting a user account

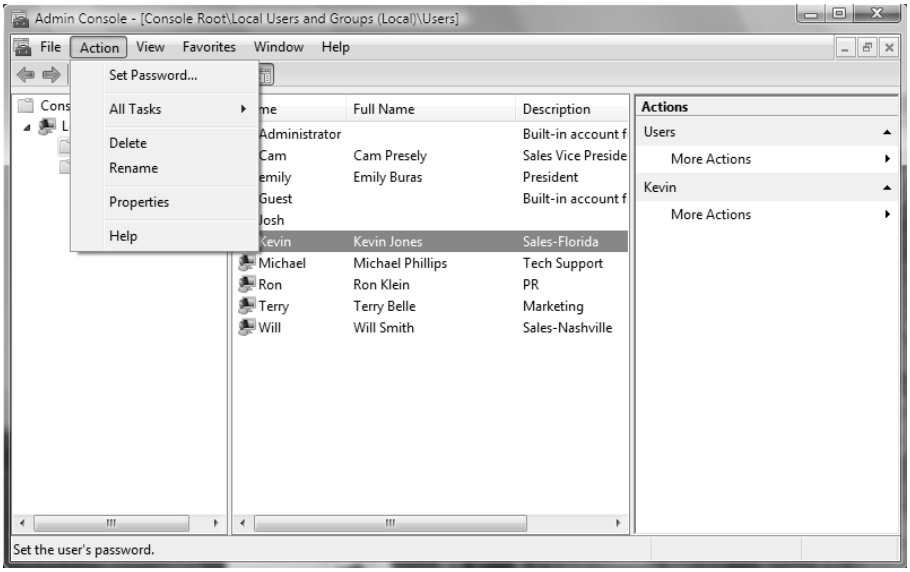
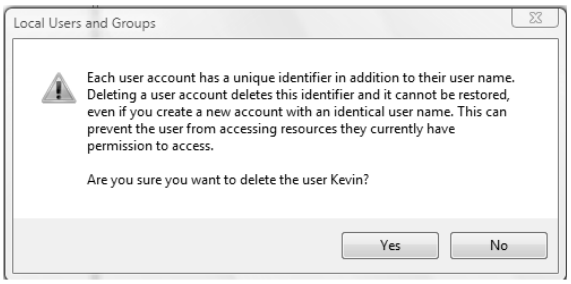


FIGURE 5.4 Confirming user deletion



EXERCISE 5.4

Deleting a User

1. Open the Admin Console MMC shortcut that was created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Expand the `Users` folder and single-click on user Kevin to select his user account.

EXERCISE 5.4 *(continued)*

3. Select Action ➢ Delete. The dialog box for confirming user deletion appears.
4. Click the Yes button to confirm that you wish to delete this user.

Renaming User Accounts

Once an account has been created, you can rename the account at any time. Renaming a user account allows the user to retain all the associated user properties of the previous username. As noted earlier in the chapter, the name is a property of the SID.

You might want to rename a user account because the user's name has changed (for example, the user got married) or because the name was spelled incorrectly. Also, as explained in the "Disabling User Accounts" section, you can rename an existing user's account for a new user, such as someone hired to take an ex-employee's position, when you want the new user to have the same properties.

In Exercise 5.5, you will rename a user account. This exercise assumes you have completed all of the previous exercises in this chapter.

EXERCISE 5.5

Renaming a User

1. Open the Admin Console MMC shortcut that was created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Open the `Users` folder and highlight user Terry.
3. Select Action ➢ Rename.
4. Type the username **Taralyn** and press Enter. Notice that the Full Name retained the original property of Terry Belle in the Local Users and Groups utility.

Renaming a user does not change any "hard-coded" names, such as the user's home folder. If you want to change these names as well, you need to modify them manually, for example, through Windows Explorer.

Changing a User's Password

What should you do if a user forgets his password and can't log on? You can't just open a dialog box and see the old password. However, as the Administrator, you can change the user's password, and then he can use the new one.

In Exercise 5.6, you will change a user's password. This exercise assumes you have completed all the previous exercises in this chapter.

EXERCISE 5.6

Changing a User's Password

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Open the `Users` folder and highlight user Ron.
3. Select Action ➢ Set Password. The Set Password dialog box appears.
4. A warning appears indicating risks involved in changing the password. Select Proceed.
5. Type the new password and then confirm the password. Click OK.

Managing User Properties

For more control over user accounts, you can configure user properties. Through the user's Properties dialog box, you can change the original password options, add the users to existing groups, and specify user profile information.

To open a user's Properties dialog box, access the Local Users and Groups utility, open the `Users` folder, and double-click the user account. The user's Properties dialog box has tabs for the three main categories of properties: General, Member Of, and Profile.

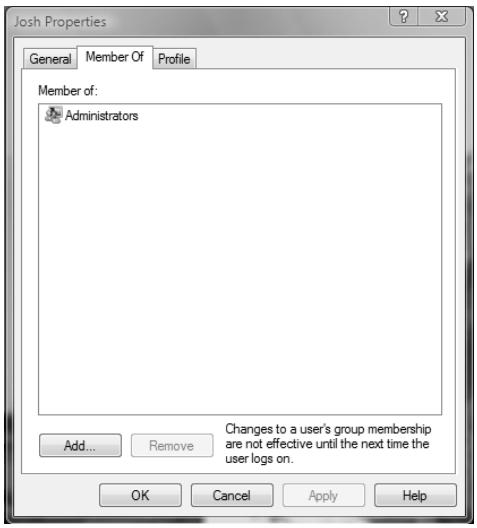
The General tab (shown in Exercise 5.3 earlier in the chapter) contains the information you supplied when you set up the new user account, including any Full Name and Description information, the password options you selected, and whether the account is disabled. (See "Creating New Users" earlier in this chapter.) If you want to modify any of these properties after you've created the user, simply open the user's Properties dialog box and make the changes on the General tab.

You can use the Member Of tab to manage the user's membership in groups. The Profile tab lets you set properties to customize the user's environment. The following sections discuss these properties in detail.

Managing User Group Membership

The Member Of tab of the user's Properties dialog box displays all the groups that the user belongs to, as shown in Figure 5.5. From this tab, you can add the user to an existing group or remove that user from a group. To add a user to a group, click the Add button and select the group that the user should belong to. If you want to remove the user from a group, highlight the group and click the Remove button.

FIGURE 5.5 The Member Of tab of the user's Properties dialog box



Groups are used to logically organize users who have similar resource access requirements. Managing groups of users is much easier than managing individual user accounts.

The steps used to add a user to an existing group are shown in Exercise 5.7. This exercise assumes you have completed all the previous exercises in this chapter.

EXERCISE 5.7

Adding a User to a Group

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Open the `Users` folder and double-click user Will. The Will Properties dialog box appears.
3. Select the Member Of tab and click the Add button. The Select Groups dialog box appears.
4. Under Enter the Object Names to Select, type **Backup Operators** and click OK.
5. Click OK to close the Will Properties dialog box.

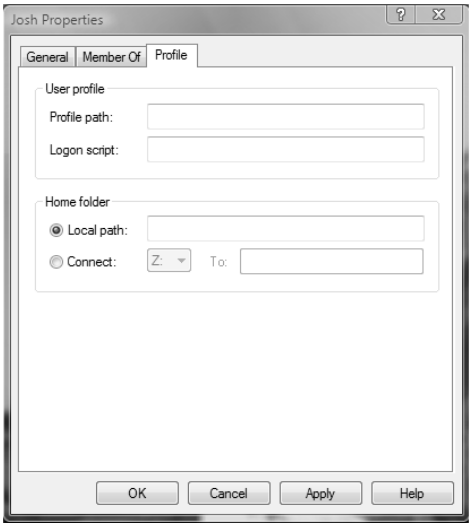
Setting Up User Profiles, Logon Scripts, and Home Folders

The Profile tab of the user's Properties dialog box, shown in Figure 5.6, allows you to customize the user's environment. Here, you can specify the following items for the user:

- User profile path
- Logon script
- Home folder

The following sections describe how these properties work and when you might want to use them.

FIGURE 5.6 The Profile tab of the user's Properties dialog box



Setting a Profile Path

User profiles contain information about the Windows Vista environment for a specific user. For example, profile settings include the Desktop arrangement, program groups, and screen colors that users see when they log on.

Each time you log on to a Windows Vista computer, the system checks to see if you have a *local user profile* in the `Users` folder, which was created on the boot partition when you installed Windows Vista.

The default location for user profiles is *systemdrive*:\Users*UserName*.

The first time users log on, they receive a default user profile. A folder that matches the user's logon name is created for the user in the `Users` folder. The user profile folder that is created holds a file called `NTUSER.DAT`, as well as subfolders that contain directory links to the user's Desktop items.

In Exercise 5.8, you will create new users and set up local user profiles.

EXERCISE 5.8

Using Local Profiles

1. Using the Local Users and Groups utility, create two new users: Tiffany and Karen. Deselect the User Must Change Password at Next Logon option for each user.
2. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer. Expand Computer, then Local Disk (C:), and then Users. Notice that the `Users` folder does not contain user profile folders for the new users.
3. Log off and log on as Tiffany.
4. Right-click an open area on the Desktop and select Personalize. In the Personalization dialog box, click Window Color and Appearance. Select the color scheme Windows Aero, click Apply, and then click OK.
5. Right-click an open area on the Desktop and select New ➢ Shortcut. In the Create Shortcut dialog box, type **CALC**. Accept CALC as the name for the shortcut and click Finish.
6. Log off as Tiffany and log on as Karen. Notice that user Karen sees the Desktop configuration stored in the default user profile.
7. Log off as Karen and log on as Tiffany. Notice that Tiffany sees the Desktop configuration you set up in steps 3, 4, and 5.
8. Log off as Tiffany and log on as your user account. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer. Expand Computer, then Local Disk (C:), and then Users. Notice that this folder now contains user profile folders for Tiffany and Karen.

If you need to reapply the default user profile for a user, you can delete the user's profile by opening the Control Panel, clicking System and Maintenance, clicking System, clicking Advanced system settings, clicking Settings in the User Profiles area of the Advanced tab, then selecting the user profile to delete and clicking Delete.

The drawback of local user profiles is that they are available only on the computer where they were created. For example, suppose all of your Windows Vista computers are a part of a domain and you use only local user profiles. User Rick logs on at Computer A and creates a customized user profile. When he logs on to Computer B for the first time, he will receive the default user profile rather than the customized user profile he created on Computer A. For users to access their user profile from any computer they log on to, you need to use roaming profiles; however, these require the use of a network server and can't be stored on a local Windows Vista computer.

In the next sections, you will learn about how roaming profiles and mandatory profiles can be used. In order to have a roaming profile or a mandatory profile, your computer must be a part of a network with server access.

Roaming Profiles

A *roaming profile* is stored on a network server and allows users to access their user profile, regardless of the client computer to which they're logged on. Roaming profiles provide a consistent Desktop for users who move around, no matter which computer they access. Even if the server that stores the roaming profile is unavailable, the user can still log on using a local profile.

Normally you would configure roaming profiles for users who are part of an Active Directory domain. In this case, you would use the Active Directory Users and Computers utility to specify the location of a user's roaming profile.

If you are using roaming profiles, the contents of the user's *systemdrive*:\Users*UserName* folder will be copied to the local computer each time the roaming profile is accessed. If you have stored large files in any subfolders of your user profile folder, you may notice a significant delay when accessing your profile remotely as opposed to locally. If this problem occurs, you can reduce the amount of time the roaming profile takes to load by moving the subfolder to another location, such as the user's home directory, or you can use Group Policy Objects within Active Directory to specify that specific folders should be excluded when the roaming profile is loaded.

Using Mandatory Profiles

A *mandatory profile* is a profile that can't be modified by the user. Only members of the Administrators group can manage mandatory profiles. You might consider creating mandatory profiles for users who should maintain consistent Desktops. For example, suppose you have a group of 20 salespeople who know enough about system configuration to make changes but not enough to fix any problems they create. For ease of support, you could use mandatory profiles. This way, all of the salespeople will always have the same profile and will not be able to change their profiles.

You can create mandatory profiles for a single user or a group of users. The mandatory profile is stored in a file named NTUSER.MAN. A user with a mandatory profile can set different Desktop preferences while logged on, but those settings will not be saved when the user logs off.

You can use only roaming profiles as mandatory profiles. Mandatory profiles do not work for local user profiles.

Using Super Mandatory Profiles

A *super mandatory profile* is a mandatory user profile with an additional layer of security. With mandatory profiles, a temporary profile is created if the mandatory profile is not available when a user logs on. However, when super mandatory profiles are configured, temporary profiles are not created if the mandatory profile is not available over the network, and the user is unable to log on to the computer. The process for creating super mandatory profiles is similar to creating mandatory profiles, except that instead of renaming the user folder to *Username*`.v2`, you name the folder as *Username*`.man.v2`.

Real World Scenario

Copying User Profiles

Within your company you have a user, Sharon, who logs in with two different user accounts. One account is a regular user account, and the other is an Administrator account used for administration tasks only.

When Sharon established all her Desktop preferences and installed the computer's applications, they were installed with the Administrator account. Now when she logs in with the regular user account, she can't access the Desktop and profile settings that were created for her as an administrative user.

To solve this problem, you can copy a local user profile from one user to another (for example from Sharon's administrative account to her regular user account) by choosing Control Panel ➢ System and Maintenance ➢ System, clicking Advanced System Settings, and clicking the User Profiles Settings button. When you copy a user profile, the following items are copied: Favorites, Cookies, Documents, Start Menu items, and other unique user Registry settings.

Using Logon Scripts

Logon scripts are files that run every time a user logs on to the network. They are usually batch files, but they can be any type of executable file.

You might use logon scripts to set up drive mappings or to run a specific executable file each time a user logs on to the computer. For example, you could run an inventory management file that collects information about the computer's configuration and sends that data to a central management database. Logon scripts are also useful for compatibility with non-Windows Vista clients who want to log on but still maintain consistent settings with their native operating system.

To run a logon script for a user, enter the script name in the Logon Script text box in the Profile tab of the user's Properties dialog box.

Logon scripts are not commonly used in Windows Server 2003 or Windows 2000 Server network environments. Windows Vista automates much of the user's configuration. This isn't the case in (for example) older Novell NetWare environments, when administrators use logon scripts to configure the users' environment.

Setting Up Home Folders

Users usually store their personal files and information in a private folder called a *home folder*. In the Profile tab of the user's Properties dialog box, you can specify the location of a home folder as a local folder or a network folder.

To specify a local path folder, choose the Local Path option and type the path in the text box next to that option. To specify a network path for a folder, choose the Connect option and specify a network path using a Universal Naming Convention (UNC) path. A UNC consists of the computer name and the share that has been created on the computer. In this case, a network folder should already be created and shared. For example, if you wanted to connect to a folder called `\Users\Will` on a server called SALES, you'd choose the Connect option, select a drive letter that would be mapped to the home directory, and then type **`\\SALES\Users\Will`** in the To box.

If the home folder you are specifying does not exist, Windows Vista will attempt to create the folder for you. You can also use the variable `%username%` in place of a specific user's name.

In Exercise 5.9, you will assign a home folder to a user. This exercise assumes you have completed all the previous exercises in this chapter.

EXERCISE 5.9

Assigning a Home Folder to a User

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Open the `Users` folder and double-click user Will. The Will Properties dialog box appears.
3. Select the Profile tab and click the Local Path radio button to select it.
4. Specify the home folder path by typing **`C:\HomeFolders\Will`** in the text box for the Local Path option. Then click OK.
5. Use Windows Explorer to verify that this folder was created.

Troubleshooting User Accounts Authentication

When a user attempts to log on through Windows Vista and is unable to be authenticated, you will need to track down the reason for the problem. The following sections offer some suggestions that can help you troubleshoot logon authentication errors for local and domain user accounts.

Real World Scenario

Using Home Folders

You are the administrator for a 100-user network. One of your primary responsibilities is to make sure that all data is backed up daily. This has become difficult because daily backup of each user's local hard drive is impractical. You have also had problems with employees deleting important corporate information as they are leaving the company.

After examining the contents of a typical user's local drive, you realize that most of the local disk space is taken by the operating system and the user's stored applications. This information does not change and does not need to be backed up. What you are primarily concerned with is backing up the user's data.

To more effectively manage this data and accommodate the necessary backup, you should create home folders for each user, stored on a network share. This allows the data to be backed up daily, to be readily accessible should a local computer fail, and to be easily retrieved if the user leaves the company.

Here are the steps to create a home folder that resides on the network. Decide which server will store the users' home folders, create a directory structure that will store the home folders efficiently (for example, `C:\HOME`), and create a single share to the home folder. Then use NTFS and share permissions to ensure that only the specified user has permissions to their home folder. Setting permissions is covered in Chapter 8. After you create the share and assign permissions, you can specify the location of the home folder through the Profile tab of the user's Properties dialog box.

Troubleshooting Local User Account Authentication

If a local user is having trouble logging on, the problem may be with the username, the password, or the user account itself. The following are some common causes of local logon errors:

Incorrect username You can verify that the username is correct by checking the Local Users and Groups utility. Verify that the name was spelled correctly.

Incorrect password Remember that passwords are case sensitive. Is the Caps Lock key on? If you see any messages relating to an expired password or locked-out account, the reason for the problem is obvious. If necessary, you can assign a new password through the Local Users and Groups utility.

Prohibitive user rights Does the user have permission to log on locally at the computer? By default, the Log On Locally user right is granted to the Users group, so all users can log on to Windows Vista computers. However, if this user right was modified, you will see an error message stating that the local policy of this computer does not allow interactive logon. The terms *interactive logon* and *local logon* are synonymous and mean that the user is logging on at the computer where the user account is stored on the computer's local database.

A disabled or deleted account You can verify whether an account has been disabled or deleted by checking the account properties through the Local Users and Groups utility.

A domain account logon at the local computer If a computer is a part of a domain, the logon dialog box has options for logging on to the domain or to the local computer. Make sure that the user has chosen the correct option.

Troubleshooting Domain User Accounts Authentication

Troubleshooting a logon problem for a user with a domain account involves checking the same areas as you do for local account logon problems, as well as a few others.

The following are some common causes of domain logon errors:

Incorrect username You can verify that the username is correct by checking the Microsoft Active Directory Users and Computers utility to verify that the name was spelled correctly.

Incorrect password As with local accounts, check that the password was entered in the proper case (and the Caps Lock key isn't on), the password hasn't expired, and the account has not been locked out. If the password still doesn't work, you can assign a new password through the Microsoft Active Directory Users and Computers utility.

Prohibitive user rights Does the user have permission to log on locally at the computer? This assumes that the user is attempting to log on to the domain controller. Regular users do not have permission to log on locally at the domain controller. The assumption is that users will log on to the domain from network workstations. If the user has a legitimate reason to log on locally at the domain controller, that user should be assigned the Log On Locally user right.

A disabled or deleted account You can verify whether an account has been disabled or deleted by checking the account properties through the Microsoft Active Directory Users and Computers utility.

A local account logon at a domain computer Is the user trying to log on with a local user account name instead of a domain account? Make sure that the user has selected to log on to a domain in the Logon dialog box.

The computer being used is not part of the domain Is the user sitting at a computer that is a part of the domain to which the user is trying to log on? If the Windows Vista computer is not

a part of the domain that contains the user account or does not have a trust relationship defined with the domain that contains the user account, the user will not be able to log on.

Unavailable domain controller, DNS server, or Global Catalog Is the domain controller available to authenticate the user's request? If the domain controller is down for some reason, the user will not be able to log on until it comes back up (unless the user logs on using a local user account). A DNS server and the Global Catalog for Active Directory are also required.

Use of the Microsoft Active Directory Users and Computers utility is covered in *MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide*.

Caching Logon Credentials

When a user login is successful, the logon credentials are saved to local cache. The next time the user attempts to log on, the cached credentials can be used to log on in the event that they can't be authenticated by a domain controller. If group policies have been updated and a user is using cached credentials, the new group policy updates will not be applied. If you want to force a user to log on using noncached credentials, you can set the number of cached credentials to 0 through a group policy.

Group Policy is covered in detail in Chapter 6.

Creating and Managing Groups

Groups are an important part of network management. Many administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users. Windows Vista includes built-in local groups, such as Administrators and Backup Operators. These groups already have all the permissions needed to accomplish specific tasks. Windows Vista also uses default special groups, which are managed by the system. Users become members of special groups based on their requirements for computer and network access.

You can create and manage local groups through the Local Users and Groups utility. With this utility, you can add groups, change group membership, rename groups, and delete groups.

Local group policies allow you to set computer configuration and user configuration options that apply to every user of the computer. Group policies are typically used with Active Directory and are applied as Group Policy Objects (GPOs). Local group policies may be useful for computers that are not part of a network or in networks that don't have a domain controller. As a

system administrator, you should understand how group policies work. In the remainder of this chapter, you will learn about all the built-in groups. Then you will learn how to create and manage groups.

Using Built-in Groups

On a Windows Vista computer, default local groups have already been created and assigned all necessary permissions to accomplish basic tasks. In addition, there are built-in special groups that the Windows Vista system handles automatically. These groups are described in the following sections.

Windows Vista, Windows XP Professional, Windows 2000 Server, and Windows Server 2003 operating systems that are installed as member servers have many of the same default groups.

Using Default Local Groups

A *local group* is a group that is stored on the local computer's accounts database. These are the groups you can add users to and can manage directly on a Windows Vista computer. By default, the following local groups are created on Windows Vista computers:

- Administrators
- Backup Operators
- Cryptographic Operators
- Distributed COM Users
- Event Log Readers
- Guests
- IIS_IUSRS
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Power Users
- Remote Desktop Users
- Replicator
- Users

We will briefly describe each group, its default permissions, and the users assigned to the group by default.

If possible, you should add users to the built-in local groups rather than creating new groups from scratch. This simplifies administration because the built-in groups already have the appropriate permissions. All you need to do is add the users whom you want to be members of the group.

The Administrators Group

The *Administrators group* has full permissions and privileges. Its members can grant themselves any permissions they do not have by default to manage all the objects on the computer. (Objects include the file system, printers, and account management.) By default, the Administrator account, which is disabled by default, and the initial user account are members of the Administrators local group.

Assign users to the Administrators group with caution since they will have full permissions to manage the computer.

Members of the Administrators group can perform the following tasks:

- Install the operating system.
- Install and configure hardware device drivers.
- Install system services.
- Install service packs, hot fixes, and Windows updates.
- Upgrade the operating system.
- Repair the operating system.
- Install applications that modify the Windows system files.
- Configure password policies.
- Configure audit policies.
- Manage security logs.
- Create administrative shares.
- Create administrative accounts.
- Modify groups and accounts that have been created by other users.
- Remotely access the Registry.
- Stop or start any service.
- Configure services.
- Increase and manage disk quotas.
- Increase and manage execution priorities.
- Remotely shut down the system.

- Assign and manage user rights.
- Reenable locked-out and disabled accounts.
- Manage disk properties, including formatting hard drives.
- Modify systemwide environment variables.
- Access any data on the computer.
- Back up and restore all data.

The Backup Operators Group

Members of the *Backup Operators group* have permissions to back up and restore the file system, even if the file system is NTFS and they have not been assigned permissions to access the file system. However, the members of Backup Operators can access the file system only through the Backup utility. To access the file system directly, Backup Operators must have explicit permissions assigned. There are no default members of the Backup Operators local group.

The Cryptographic Operators Group

The *Cryptographic Operators group* has access to perform cryptographic operations on the computer. There are no default members of the Cryptographic Operators local group.

The Distributed COM Users Group

The *Distributed COM Users group* has the ability to launch and run Distributed COM objects on the computer. There are no default members of the Distributed COM Users local group.

The Event Log Readers Group

The *Event Log Readers group* has access to read the event log on the local computer. There are no default members of the Event Log Readers local group.

The Guests Group

The *Guests group* has limited access to the computer. This group is provided so that you can allow people who are not regular users to access specific network resources. As a general rule, most administrators do not allow Guest access because it poses a potential security risk. By default, the Guest user account is a member of the Guests local group.

The IIS_IUSRS Group

The *IIS_IUSRS group* is used by Internet Information Services (IIS). The NT AUTHORITY\IUSR user account is a member of the IIS_IUSRS group by default.

The Network Configuration Operators Group

Members of the *Network Configuration Operators group* have some administrative rights to manage the computer's network configuration—for example, editing the computer's TCP/IP settings.

The Performance Log Users Group

The *Performance Log Users group* has the ability to access and schedule logging of performance counters and can create and manage trace counters on the computer.

The Performance Monitor Users Group

The *Performance Monitor Users group* has the ability to access and view performance counter information on the computer. Users who are members of this group can access performance counters both locally and remotely.

The Power Users Group

The *Power Users group* is included in Windows Vista for backward compatibility. The Power Users group is included to ensure that computers upgraded from Windows XP function as before with regard to folders that allow access to members of the Power Users group. Otherwise, the Power Users group has limited administrative rights.

The Remote Desktop Users Group

The *Remote Desktop Users group* allows members of the group to log on remotely for the purpose of using the Remote Desktop service.

The Replicator Group

The *Replicator group* is intended to support directory replication, which is a feature used by domain servers. Only domain users who will start the replication service should be assigned to this group. The Replicator local group has no default members.

The Users Group

The *Users group* is intended for end users who should have very limited system access. If you have installed a fresh copy of Windows Vista, the default settings for the Users group prohibit its members from compromising the operating system or program files. By default, all users who have been created on the computer, except Guest, are members of the Users local group.

An efficient function for the Users group is to allow users to run but not modify installed applications. Users should not be allowed general access to the file system.

Using Special Groups

Special groups are used by the system. Membership in these groups is automatic if certain criteria are met. You cannot manage special groups through the Local Users and Groups utility. Table 5.2 describes several of the special groups that are built into Windows Vista.

TABLE 5.2 Special Groups in Windows Vista

Group	Description
Creator Owner	The account that created or took ownership of the object. This is typically a user account. Each object (files, folders, printers, and print jobs) has an owner. Members of the Creator Owner group have special permissions to resources. For example, if you are a regular user who has submitted 12 print jobs to a printer, you can manipulate your print jobs as Creator Owner, but you can't manage any print jobs submitted by other users.
Everyone	The group that includes anyone who could possibly access the computer. The Everyone group includes all users who have been defined on the computer (including Guest), plus (if your computer is a part of a domain) all users within the domain. If the domain has trust relationships with other domains, all users in the trusted domains are part of the Everyone group as well. The exception to automatic group membership with the Everyone group is that members of the Anonymous Logon group are not included as a part of the Everyone group.
Interactive	The group that includes all users who use the computer's resources locally. Local users belong to the Interactive group.
Network	The group that includes users who access the computer's resources over a network connection. Network users belong to the Network group.
Authenticated Users	The group that includes users who access the Windows Vista operating system through a valid username and password. Users who can log on belong to the Authenticated Users group.
Anonymous Logon	The group that includes users who access the computer through anonymous logons. When users gain access through special accounts created for anonymous access to Windows Vista services, they become members of the Anonymous Logon group.
Batch	The group that includes users who log on as a user account that is used only to run a batch job. Batch job accounts are members of the Batch group.
Dialup	The group that includes users who log on to the network from a dial-up connection. Dial-up users are members of the Dialup group.
Service	The group that includes users who log on as a user account that is used only to run a service. You can configure the use of user accounts for logon through the Services program (discussed in Chapter 3), and these accounts become members of the Service group.

TABLE 5.2 Special Groups in Windows Vista *(continued)*

Group	Description
System	When the system accesses specific functions as a user, that process becomes a member of the System group.
Terminal Server User	The group that includes users who log on through Terminal Services. These users become members of the Terminal Server User group.

Working with Groups

Groups are used to logically organize users with similar rights requirements. Groups simplify administration because you can manage a few groups rather than many user accounts. For the same reason, groups simplify troubleshooting. Users can belong to as many groups as needed, so it's not difficult to put users into groups that make sense for your organization.

For example, suppose Jane is hired as a data analyst, to join the four other data analysts who work for your company. You sit down with Jane and create an account for her, assigning her the network permissions for the access you think she needs. Later, however, you find that the four other data analysts (who have similar job functions) sometimes have network access Jane doesn't have, and sometimes she has access they don't have. This is happening because all their permissions were assigned individually and months apart. To avoid such problems and reduce your administrative workload, you can assign all the company's data analysts to a group and then assign the appropriate permissions to that group. Then, as data analysts join or leave the department, you can simply add them to or remove them from the group.

You can create new groups for your users, and you can use the Windows Vista default local built-in groups that were described in the previous section. In both cases, your planning should include checking to see if an existing local group meets your requirements before you decide to create a new group. For example, if all the users need to access a particular application, it makes sense to use the default Users group rather than creating a new group and adding all the users to that group.

To work with groups, you can use the Local Users and Groups utility.

Creating Groups

To create a group, you must be logged on as a member of the Administrators group. The Administrators group has full permissions to manage users and groups.

As you do in your choices for usernames, keep your naming conventions in mind when assigning names to groups. When you create a local group, consider the following guidelines:

- The group name should be descriptive (for example, Accounting Data Users).

- The group name must be unique to the computer, different from all other group names and usernames that exist on that computer.
- Group names can be up to 256 characters. It is best to use alphanumeric characters for ease of administration. The backslash (\) character is not allowed.

Creating groups is similar to creating users, and it is a fairly easy process. After you've added the Local Users and Groups snap-in to the MMC, expand it to see the `Users and Groups` folders. Right-click the `Groups` folder and select New Group from the context menu. This brings up the New Group dialog box, shown in Figure 5.7.

The only required entry in the New Group dialog box is the group name. If appropriate, you can enter a description for the group, and you can add (or remove) group members. When you're ready to create the new group, click the Create button.

In Exercise 5.10, you will create two new local groups.

FIGURE 5.7 The New Group dialog box

EXERCISE 5.10

Creating Local Groups

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Right-click the `Groups` folder and select New Group.
3. In the New Group dialog box, type **Data Users** in the Group Name text box. Click the Create button.
4. In the New Group dialog box, type **Application Users** in the Group Name text box. Click the Create button.

Managing Group Membership

After you've created a group, you can add members to it. As mentioned earlier, you can put the same user in multiple groups. You can easily add and remove users through a group's Properties dialog box, shown in Figure 5.8. To access this dialog box from the `Groups` folder in the Local Users and Groups utility, double-click the group you want to manage.

From the group's Properties dialog box, you can change the group's description and add or remove group members. When you click the Add button to add members, the Select Users dialog box appears (Figure 5.9). Here, you enter the object names of the users you want to add. You can use the Check Names button to validate the users against the database. Select the user accounts you wish to add and click Add. Click the OK button to add the selected users to the group. (Although the special groups that were covered earlier in the chapter are listed in this dialog box, you cannot manage the membership of these special groups.)

FIGURE 5.8 A group Properties dialog box

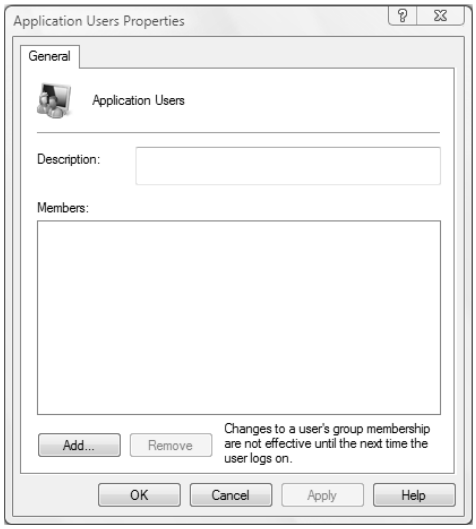
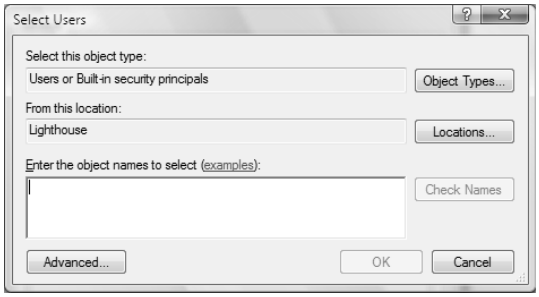


FIGURE 5.9 The Select Users dialog box



To remove a member from the group, select the member in the Members list of the Properties dialog box and click the Remove button.

In Exercise 5.11, you will create new user accounts and then add these users to one of the groups you created in Exercise 5.10.

EXERCISE 5.11

Adding Users to a Local Group

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Create two new users: **Joe** and **David**. Deselect the User Must Change Password at Next Logon option for each user.
3. Expand the Groups folder.
4. Double-click the Data Users group (created in Exercise 5.10).
5. In the Data Users Properties dialog box, click the Add button.
6. In the Select Users dialog box, type the username **Joe**, then click OK. Click Add and type the username **David**, then click OK.
7. In the Data Users Properties dialog box, you will see that the users have all been added to the group. Click OK to close the group's Properties dialog box.

Renaming Groups

Windows Vista provides an easy mechanism for changing a group's name. For example, you might want to rename a group because its current name does not conform to existing naming conventions.

As happens when you rename a user account, a renamed group keeps all of its properties, including its members and permissions.

To rename a group, right-click the group and choose Rename from the context menu. Enter a new name for the group and press Enter.

In Exercise 5.12, you will rename one of the groups you created in Exercise 5.10.

EXERCISE 5.12

Renaming a Local Group

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Expand the Groups folder.

EXERCISE 5.12 *(continued)*

3. Right-click the Data Users group (created in Exercise 5.10) and select Rename.
4. Rename the group to **App Users** and press Enter.

Deleting Groups

If you are sure that you will never again want to use a particular group, you can delete it. Once a group is deleted, you lose all permissions assignments that have been specified for the group.

To delete a group, right-click the group and choose Delete from the context menu. You will see a warning that once a group is deleted, it is gone for good. Click the Yes button if you're sure you want to delete the group.

If you delete a group and give another group the same name, the new group won't be created with the same properties as the deleted group.

In Exercise 5.13, you will delete the group that you created in Exercise 5.10 and renamed in Exercise 5.12.

EXERCISE 5.13

Deleting a Local Group

1. Open the Admin Console MMC shortcut you created in Exercise 5.1 and expand the Local Users and Groups snap-in.
2. Expand the Groups folder.
3. Right-click the App Users group and choose Delete.
4. In the dialog box that appears, click Yes to confirm that you want to delete the group.

Summary

In this chapter, you learned about user-management features in Windows Vista. We covered the following topics:

- The types of accounts supported by Windows Vista. You can set up local user accounts and domain user accounts.
- The user logon and logoff processes. To log on to a Windows Vista computer, the user must supply a username and password, with which the system authenticates the user.

- The procedures for creating and managing user accounts. You create user accounts and manage them through the Local Users and Groups utility or through the User Accounts and Family Settings option in the Control Panel.
- What user properties are and how they can be configured for user accounts. The General tab of the user's Properties dialog box allows you specify logon, password, and whether an account is disabled. On the Member Of tab, you can add users to groups or remove them from group membership. The Profile tab lets you set a profile path, logon script, and home folder for the user.
- Troubleshooting user logon and authentication problems. Some of the problems you may encounter are incorrect usernames or passwords, prohibitive user rights, and disabled or deleted accounts.
- The Windows Vista built-in groups, which include default local groups such as Administrators and Power Users, and default special groups such as Everyone and Network. You can manage the default local groups, but the special groups are managed by the system.
- The procedure for creating groups. You can create groups through the Local Users and Groups utility.
- The procedure for adding users to groups and removing users from groups. You perform these tasks via the group's Properties dialog box.
- Renaming and deleting groups. Both of these tasks are performed by right-clicking the group in the `Groups` folder of the Local Users and Groups utility and selecting the appropriate option from the context menu.

Exam Essentials

Be able to create and manage user accounts. When creating user accounts, be aware of the requirements for doing so. Understand User Account Control. Know how to rename and delete user accounts. Be able to manage all user properties.

Know how to configure and manage local user authentication. Understand the options that can be configured to manage local user authentication and when these options would be used to create a more secure environment. Be able to specify where local user authentication options are configured.

Be able to set up a security configuration based on network requirements. Define the options that can be configured for secure network environments. Know where to configure each option.

Know how to manage local groups. Understand the local groups that are created on Windows Vista computers by default, and be familiar with the rights each group has. Know how to create and manage new groups.

Review Questions

1. You are the network administrator for a medium-sized company. A user, John, has created a local profile on his Windows Vista computer that now contains some corrupted settings. You want to look at his profiles folder and delete the corrupted information. His computer was initially installed with Windows Vista. Where are user profiles stored by default on this computer?

   A. `\WINNT\Profiles\`*`username`*

   B. *`systemdrive:`*`\Users\`*`username`*

   C. `\WINNT\User Profiles\`*`username`*

   D. *`systemdrive:`*`\Documents and Settings\`*`username`*

2. You are the system administrator for the BrainBeacon network. One of your users, Bill, uses two different Windows Vista computers. He wants to be able to use his user profile from either computer. Which of the following steps would you need to take to specify that a user profile is available over the network for a Windows Vista client?

   A. In Control Panel, on the User Profiles tab of the System Properties dialog box, specify that the profile is a roaming profile.

   B. Rename the user profile to **`NTUSER.NET`**.

   C. Use Windows Explorer to copy the user profile to a network share.

   D. In the Local Users and Groups utility, in the Profile tab of the user's Properties dialog box, specify a UNC path for the roaming profile.

3. Rob is the network administrator of a large company. The company requires that all Sales users use a profile that has been specified by the IT department as the corporate standard. Rob has been having problems because users in the Sales group are changing their profiles so that they are no longer using the corporate-defined standard. Which of the following steps should Rob take to create a mandatory profile in Windows Vista? (Choose all that apply.)

   A. In Control Panel, in the User Profiles dialog box, specify that the profile is a mandatory profile.

   B. Rename the user profile to **`NTUSER.MAN`**.

   C. Copy the profile to a network share using the User Profiles dialog box accessible from the System Properties dialog box in Control Panel.

   D. In the Local Users and Groups utility, on the Profile tab of the user's Properties dialog box, specify a UNC path for the roaming profile.

4. Sean works in the IT department, where all of the Windows Vista computers have been configured in a workgroup called IT. You want him to be able to create users and groups on the Windows Vista computers within the workgroup. To which of the following groups should you add Sean on each Windows Vista computer he will manage?

   A. Administrators

   B. Power Users

   C. Server Operators

   D. Power Operators

5. Rick has been added to the Administrators group, but you suspect that he is abusing his administrative privileges. All he really needs permission for is viewing event information and scheduling logging of performance counters. To which group or groups should you add Rick so that he can do his job but will have the minimum level of administrative rights? (Choose all that apply.)

   A. Administrators

   B. Power Users

   C. Event Log Readers

   D. Performance Log Users

   E. Performance Monitor Users

6. You are logged on as a member of the Administrators group on a Windows Vista computer. You are adding a new user account to the computer. You want to create a temporary password that the user must change, and you want to ensure that the account is enabled. Which of the following options should you configure? (Choose all that apply.)

   A. User Must Change Password at Next Logon

   B. User Cannot Change Password

   C. Password Never Expires

   D. Account Is Disabled

7. Ben has just installed Windows Vista. No changes have been made to the default user accounts. He is trying to determine if any of the default account assignments pose a security threat. Which of the following statements are true regarding the built-in accounts? (Choose all that apply.)

   A. By default, the Administrator account cannot be deleted.

   B. By default, the Guest account cannot be deleted.

   C. By default, the Administrator account is enabled.

   D. By default, the Guest account is enabled.

8. You are the network administrator of a small network. None of the users' local computers' data is backed up for recovery purposes. Only data that is stored on the network servers is backed up on a daily basis. One of your users, Dionne, needs to have her critical data backed up daily. She decides to create a home folder that will be used in conjunction with offline folders. Which option should she select within the Profile tab of User Properties to create a home folder that was located on a network path?

   A. Connect

   B. Local path

   C. Network path

   D. Connect path

9. You are the network administrator for a medium-sized company. Rick was the head of HR and recently resigned. John has been hired to replace Rick and has been given Rick's laptop. You want John to have access to all of the resources to which Rick had access. What is the easiest way to manage the transition?

   A. Rename Rick's account to John.

   B. Copy Rick's account and call the copied account John.

   C. Go into the Registry and do a search and replace to replace all of Rick's entries with John's name.

   D. Take ownership of all of Rick's resources and assign John Full Control to the resources.

10. You are the system administrator for a large network. One of your remote users, Brett, needs to make sure that his files are backed up on a daily basis. You install a tape backup drive on Brett's laptop. You make Brett a member of the Backup Operators group for his computer. Which of the following statements about the Backup Operators group is true?

    A. By default, only Administrators can be members of the Backup Operators group.

    B. Backup Operators do not require any additional permissions to NTFS file systems to back up and restore the file system.

    C. Backup Operators have full access to the NTFS file system.

    D. Backup Operators can modify any services that relate to system backup.

11. If you log on as user Brad to a Windows Vista computer that contains the user account Brad, which of the following groups will you belong to by default? (Choose all that apply.)

    A. Users

    B. Authenticated Users

    C. Everyone

    D. Interactive

12. When Beth logs on to the Windows Vista computer named Sales1, she sees her normal Desktop. When Beth logs on to a Windows Vista computer named Sales2, she does not see her normal Desktop. What is the most likely cause?

    A. A roaming user profile is not configured for Beth.

    B. Beth does not have permissions to access her user profile from Sales2.

    C. Beth has a mandatory profile configured in Sales2.

    D. The computer at which Beth is logging on is a Windows NT 4 computer.

13. You want to allow Sarah to create and manage the mandatory profiles that are used by the sales department. Which of the following group memberships would allow her to manage mandatory user profiles?

    A. The user to whom the profile is assigned

    B. The Administrators group

    C. The Power Users group

    D. The Server Operators group

14. Nicky and Jaime share the same Windows Vista computer. Nicky has configured a Desktop that Jaime would like to use. How can you configure Jaime's user profile so that it will initially match Nicky's settings?

    A. Copy the `NTUSER.DAT` file from Nicky's folder to Jaime's folder.

    B. Configure a roaming profile that will be used by both users.

    C. Copy Nicky's user profile to Jaime's folder in the `Users` folder (using Control Panel ➢ System and Maintenance ➢ System ➢ Advanced System Settings, selecting the Advanced tab, and clicking the Settings button in the User Profiles area). Configure the profile so that Jaime is permitted to use the copied profile.

    D. Copy Nicky's user profile to Jaime's folder in the `Profiles` folder (using Control Panel ➢ System and Maintenance ➢ System ➢ Advanced System Settings, selecting the Advanced tab, and clicking the Settings button in the User Profiles area).

15. Christine wants to connect her home folder to a shared folder that exists in the workgroup SALES, on a computer called DATA, and on a share called Users. Christine has full access to this folder and share. She also wants to use a variable for her username when she specifies the path to the network folder. Which of the following options should Christine use?

    A. On the Profile tab of Christine's User Properties, she should click the Connect button and specify the path as **`\\SALES\DATA\Users\%logonname%`**.

    B. On the Profiles tab of Christine's User Properties, she should click the Connect button and specify the path as **`\\SALES\DATA\Users\%username%`**.

    C. On the Profile tab of Christine's User Properties, she should click the Connect button and specify the path as **`\\DATA\Users\%logonname%`**.

    D. On the Profile tab of Christine's User Properties, she should click the Connect button and specify the path as **`\\DATA\Users\%username%`**.

16. You are a systems administrator for a small organization. Three employees are currently responsible for performing many of the marketing tasks and often need to share computers. Each of the marketing employees' user accounts has been assigned the appropriate permissions on the computers. A new employee named George has been hired to help with the marketing tasks and her user account will need similar permissions as the other marketing employees. Which of the following should you do to provide George with the appropriate level of permissions?

A. Rename one of the other marketing user accounts to George, and provide George with access to that account.

B. Copy one of the existing marketing user accounts and assign George permission to the new account.

C. Assign George to the Administrators group.

D. Create a new group named Marketing, add all of the marketing users to the Marketing group, and assign the Marketing group the appropriate permissions.

17. You are a network administrator for your company. Your company has implemented several password policies to increase the security associated with user accounts. A user has called you and indicated that he can no longer log into his user account. He indicates that he has tried typing the password several times and now is getting an error message. You need to allow the user to log on using his user account. Which of the following should you do?

A. Delete the user account and create a new account. Instruct the user to log on using a temporary password.

B. Open the user's Properties dialog box, and deselect the Account Is Disabled option.

C. Reset the user's password.

D. Open the user's Properties dialog box, and deselect the Account Is Locked Out option.

18. You are the system administrator for your company. You are configuring a new Windows Vista computer that will be shared among several supervisors in the manufacturing department. Two of the users are named Nick R. Smith and Nancy L. Smith, and you need to create user accounts for both users that conform to your company's naming conventions, which typically use the user's first initial followed by the last name. Which of the following should you do?

A. For one account, capitalize the first initial, Nsmith, and for the other account, leave all letters lowercase, nsmith.

B. Use the same username but different passwords.

C. Use the middle initial in addition to the first initial.

D. Use both users' full names.

19. You are configuring a new Windows Vista computer that will be used by a new employee. The new employee is a member of the HR department and will require access to a group of folders that will be copied to the computer. You create a group called HR on the computer and assign the HR group the rights to the folders. You now need to add the new user to the group. How could you accomplish this task? (Choose all that apply.)

A. On the Member Of tab of the user's Properties dialog box, click Add and add the group to the user account.

B. On the General tab of the user's Properties dialog box, click Add and add the group to the user account.

C. On the General tab of the group's Properties dialog box, click Add to add the user to the group.

D. On the Members tab of the group's Properties dialog box, click Add to add the user to the group.

20. You are a system administrator for your company. The company has recently fired an employee named Tim, and you want to ensure that Tim is not able to log on to his computer and access company resources. Which of the following should you do?

A. Remove Tim's user account from any groups to which he belonged.

B. Delete Tim's user account.

C. Create a group named ExEmployees and assign Tim's user account as a member of the new group.

D. Deselect the Password Never Expires option on Tim's user account properties dialog box.

Answers to Review Questions

1. B. The default location for user profiles is the *systemdrive:*\Users*username* folder in Windows Vista. Windows 2000 and Windows XP stored user profiles at *systemdrive:*\Documents and Settings*username*. In Windows NT 4, the default location for user profiles was \WINNT\Profiles.

2. D. After you create the profile that will be used as the roaming profile, you create a folder and share on the network location where the roaming profile will be stored. You first select Control Panel ➢ System and Maintenance ➢ System ➢ Advanced System Settings; then in the System Properties dialog box, select the Advanced tab and click the Settings button in the User Profiles area to copy the local profile to the network share. Finally, you specify that the user is using a roaming profile by configuring the user's properties through the Local Users and Groups utility. On the Profile tab, you specify a UNC path for the roaming profile.

3. B, C, D. Creating a mandatory profile involves three main steps. First, rename the user profile from NTUSER.DAT to **NTUSER.MAN**. Second, copy the profile to a network share using Control Panel ➢ System and Maintenance ➢ System ➢ Advanced System Settings; then in the System Properties dialog box select the Advanced tab and click Settings button in the User Profiles area. Third, in the Local Users and Groups utility, access the properties of the user who will be assigned the roaming profile, and specify the location of the mandatory profile. This path must be a UNC path for the mandatory profile to work.

4. A. Members of the Administrators group have full control over the computer and, thus, can create users and groups. The Power Users group is included in Windows Vista for backward compatibility and has minimal administrative rights. The Server Operators group exists only on Windows 2000 and Windows 2003 domain controllers. The Power Operators group does not exist by default on Windows Vista computers.

5. C, D. The members of the Event Log Readers group have the ability to read event logs on the local machine. Members of the Performance Log Users group have the ability to schedule logging of performance counters and to enable trace providers. Therefore, it is not necessary for Rick to be a member of the Administrators group, because he can perform his job as a member of both the Event Log Readers group and the Performance Log Users group. The Power Users group is included in Windows Vista for backward compatibility and has limited administrative rights on Windows Vista. The members of the Performance Monitor Users groups have permission to access performance monitor data.

6. A. To configure a temporary password that the user must change, you can select the User Must Change Password at Next Logon option in the New User dialog box. By configuring this option, the user will be required to change their password when they first log on to the computer.

7. A, B. By default, the Administrator and Guest accounts cannot be deleted, although they can both be renamed. Both the Administrator account and the Guest account are disabled by default. It is strongly recommended that you use a complex password for the Administrator account if it is enabled.

8. A. The Connect option on the Home folder area of the Profile tab of the user's Properties dialog box should be used to specify a network location where the home folder is located.

9. A. The easiest way to manage this transition is to simply rename Rick's account to John. John will automatically have all of the rights and permissions to any resource that Rick had access to.

10. B. There are no default members of the Backup Operators group. Members of this group have access to the file system during the backup process, but they do not have normal file access. Backup Operators group members have no special permissions to modify system services.

11. A, B, C, D. By default, all users who exist on a Windows Vista computer are added to the computer's Users group. Users who log on with a valid username and password automatically become a member of the Authenticated Users special group. By default, anyone who can use the computer becomes a member of the special group Everyone. Since Brad works at the computer where his user account actually resides, he automatically becomes a member of the special group Interactive.

12. A. By default, profiles are configured only to be used locally. In this case, it is likely that no roaming profile has been configured for Beth.

13. B. Only members of the Administrators group can create and assign mandatory user profiles.

14. C. You can copy Nicky's user profile so that Jaime can use it initially by copying Nicky's user profile to Jaime's folder in the `Users` folder. You can perform this copy operation by choosing Control Panel ➢ System and Maintenance ➢ System ➢ Advanced System Settings, selecting the Advanced tab, and clicking the Settings button in the User Profiles area.

15. D. To connect to a shared network folder for a user's home folder, you must use the UNC path to the share. In this case, Christine would specify `\\DATA\Users`. The variable that can be used is *`%username%`*.

16. D. You should create a new group named Marketing, assign each member of the marketing department to the Marketing group, and ensure that the Marketing group has the appropriate level of permissions. Managing groups is typically easier than managing rights on individual user accounts, particularly when those user accounts require a similar level of access to resources.

17. D. You should Open the user's Properties dialog box, and deselect the Account Is Locked Out option. The most likely scenario is that the user has exceeded the maximum number of logon attempts allowed by your company's password policy. As a result, the user's account will be locked out until reset by an administrator. Deselecting the Account Is Locked Out option should enable the user to log on using his original username and password.

18. C. You should use the middle initial in addition to the first initial. For example, Nick's user account would be nrsmith, and Nancy's user account would be nlsmith. These user accounts would conform to your company's naming convention and would not conflict with each other. Usernames are not case sensitive, so capitalizing one and leaving one lowercase would create a conflict between the accounts. Although you could use both users' full names, doing so may not conform to your company's naming conventions, whereas the first initial and middle initial combination would most likely conform to your company's naming convention.

19. A, C. You could add the user to the HR group in the following ways. You could open the user's Properties dialog box and click the Member Of tab, then click the Add button to assign the user to the HR group. Or, you could click Add to add the user to the group on the General tab of the group's Properties dialog box.

20. B. When an employee's user account is no longer needed, such as when the employee leaves the organization, you should delete the user account from the system to ensure that the user is not able to log back on to the computer and access company resources. You could also disable the user account to prevent the user from logging on, but it is more secure to delete the user account if it is no longer needed.

Chapter

6

Configuring Security

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring Windows Security Features**
  - Configure and troubleshoot User Account Control
  - Configure Windows Defender
  - Configure security settings in Windows Firewall

Windows Vista offers a wide variety of security options. If the Windows Vista computer is a part of a Windows 2000 or Windows 2003 domain, then you can apply security through a Group Policy within Active Directory. If the Windows Vista computer is not a part of a Windows 2000 or Windows 2003 domain, then you use Local Group Policy Objects to manage local security. In the first part of this chapter, you will learn about the different environments that Windows Vista can be installed in and the utilities that are used to manage security.

You can use *policies* to help manage user accounts. Account policies control the logon environment for the computer, such as password and logon restrictions. Local policies specify what users can do once they log on and include auditing, user rights, and security options. You can also manage critical security features through the Windows Security Center.

Options for Managing Security Configurations

The tools you use to manage Windows Vista computer security configurations depend on whether the Windows Vista computer is a part of a Windows 2000 or Windows 2003 domain environment.

If the Windows Vista client is not a part of a Windows 2000 or Windows 2003 domain—for example, if the computer is installed as a stand-alone computer or part of a Windows workgroup, Windows NT 4 domain, Unix network, or Novell NetWare network—then you apply security settings through *Local Group Policy Objects (LGPOs)*. LGPOs are a set of security configuration settings that are applied to users and computers. LGPOs are created and stored on the Windows Vista computer.

If your Windows Vista computer is a part of a Windows 2000 Server or Windows Server 2003 domain, both of which use the services of *Active Directory*, then you typically manage and configure security through *Group Policy Objects (GPOs)*. The Group Policy Management Tool is an MMC snap-in that is used to define security (called *group policies*) for users, groups, and computers via Active Directory. Windows Vista computers that are part of a Windows 2000 or Windows 2003 domain still have LGPOs, and you can use LGPOs in conjunction with the Active Directory group policies.

Usage of Group Policy Objects is covered in greater detail in *MCSA/MCSE: Windows Server 2003 Environment Management and Maintenance Study Guide: Exam 70-290*, by Lisa Donald with James Chellis (Sybex, 2006).

The settings you can apply through the Group Policy utility within Active Directory are more comprehensive than the settings you can apply through LGPOs. By default, LGPOs are stored in `\systemroot\System32\GroupPolicyUsers`. Table 6.1 lists all of the options that can be set for GPOs within Active Directory and which of those options can be applied through LGPOs.

TABLE 6.1 Group Policy and LGPO Setting Options

Group Policy Setting	Available for LGPO?
Software installation	No
Remote Installation Services	Yes
Scripts	Yes
Printers	Yes
Security settings	Yes
Policy-based QOS	Yes
Administrative templates	Yes
Folder redirection	No
Internet Explorer configuration	Yes

Group Policy Objects and Active Directory

Most Windows Vista computers reside within Windows 2000 domains or Windows 2003 domains. Typically, GPOs are applied through Active Directory, because this is much easier to globally manage than applying LGPOs at local levels. To help you understand how GPOs and LGPOs work together, the following sections will first provide an overview of Active Directory and then show you how GPOs and LGPOs are applied based on predefined inheritance rules.

Active Directory Overview

Within Active Directory, you have several levels of hierarchical structure. A typical structure will consist of domains and *Organizational Units (OUs)*. Other levels exist within Active Directory, but this overview focuses on domains and OUs in the context of using GPOs.

The *domain* is the main unit of organization within Active Directory. Within a domain are many domain objects (including users, groups, and GPOs). Each domain object can have security applied that specifies who can access the object and the level of access they have.

Within a domain, you can further subdivide and organize domain objects through the use of Organizational Units. This is one of the key differences between Windows NT 3.51 and Windows NT 4 domains, and Windows 2000 Server and Windows Server 2003 domains. The NT domains were not able to store information hierarchically. Windows 2000 Server and Windows Server 2003 domains, through the use of OUs, allow you to store objects hierarchically, typically based on function or geography.

For example, assume that your company is called ABCCORP. You have locations in New York, San Jose, and Belfast. You might create a domain called ABCCORP.COM with OUs called NY, SJ, and Belfast. In a very large corporation, you might also organize the OUs based on function. For example, the domain could be ABCCORP.COM and the OUs might be SALES, ACCT, and TECHSUPP. Based on the size and security needs of your organization, you might also have OUs nested within OUs. As a general rule, however, you will want to keep your Active Directory structure as simple as possible.

GPO Inheritance

When GPOs are created within Active Directory, there is a specific order of inheritance. That is, the policies are applied in a specific order within the hierarchical structure of Active Directory. When a user logs onto Active Directory, depending on where within the hierarchy GPOs have been applied, the order of application is as follows:

1. Local
2. Site (physical location)
3. Domain
4. OU

Each level of the hierarchy is called a container. Containers higher in the hierarchy are called parent containers; containers lower in the hierarchy are called child containers. Settings from these containers are inherited from parent container to child container. By default, child container policy settings override any conflicting settings applied by parent containers.

The local policy is, by default, applied first when a user logs on. Then the site policies are applied, and if the site policy contains settings that the local policy doesn't have, they are added to the local policy. If there are any conflicts, the site policy overrides the local policy. Then the domain policies are defined. Again, if the domain policy contains additional settings, they are incorporated. When settings conflict, the domain policy overrides the site policy or local policy. Finally, the OU policies are applied. Any additional settings are incorporated; for conflicts, the OU policy overrides the domain, site, and local policies. If any child OUs exist, their GPOs are applied after the parent OU GPOs.

Two types of policy settings exist: computer settings and user settings. If conflicts occur between computer and user policy settings, the computer policy setting is applied.

The following options are available for overriding the default behavior of GPO execution:

No Override The No Override option is used to specify that child containers can't override the policy settings of higher-level containers. For example, if a site policy is marked as No Override, it will not be overridden by conflicting domain or OU policies. If multiple No Override policies are set, then the one from the highest container would take precedence. The No Override option would be used if you wanted to set corporate-wide policies without allowing administrators of lower-level containers to override your settings. This option can be set per container, as needed.

Block Inheritance The Block Inheritance option is used to allow a child container to block GPO inheritance from parent containers. This option would be used if you do not want to inherit GPO settings from parent containers and want only the GPO you have set for your container to be applied. For example, if you set Block Inheritance on an OU policy, only the OU policy would be applied; no parent container policies would be inherited.

If a conflict exists between the No Override and the Block Inheritance settings, then the No Override option would be applied.

Applying GPOs

You manage a network that consists of 500 computers all running Windows Vista. You are already using Active Directory and have logically defined your OUs based on function. One OU, called Sales, has 50 users. Your task is to configure the Sales computers so they all have a consistent Desktop that can't be modified. You also need to add the new Sales Management software to each computer.

It would take days for you to manually configure each computer with a local group policy and then add the software. In this case, GPOs are a real benefit. As the Administrator of the Sales OU, you can create a single GPO that will be applied to all users of the container. You can specify the Desktop settings and publish any applications that you want to install. Next time the Sales users log on, the group policies will be applied, and the users' Registries will be updated to reflect the changes. In addition, through the automated publishing applications, it can be configured to be automatically loaded on each of the Sales users' computers.

By using GPOs, you can add new software, configure computers, and accomplish other tasks from your computer that would normally require you to physically visit each machine.

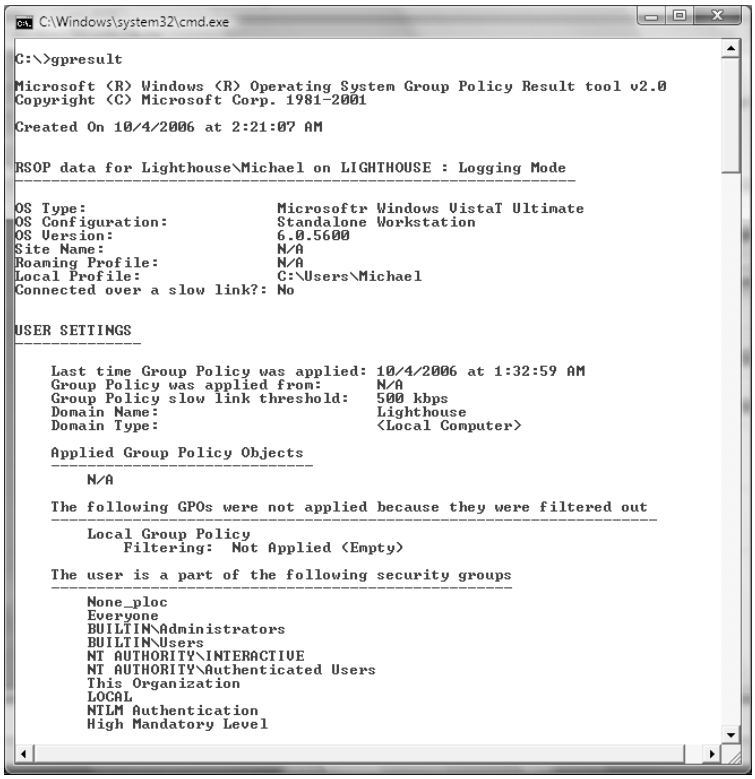
Using the Group Policy Result Tool

When a user logs on to a computer or domain, a resulting set of policies to be applied is generated based on the LGPOs, site GPOs, domain GPOs, and OU GPOs. The overlapping nature of group policies can make it difficult to determine what group policies will actually be applied to a computer or user.

To help determine what policies will actually be applied, Windows Vista includes a tool called the Windows Operating System *Group Policy Result Tool*. You can access this tool through the GPResult command-line utility. The `gpresult` command displays the resulting set of policies that were enforced on the computer and the specified user during the logon process, as shown in Figure 6.1.

You can use this utility by accessing a command prompt and typing **`gpresult`**. This will display the Resultant Set of Policy (RSOP) for the computer and user who is currently logged in. Several options can be used with this command. Use **`gpresult /?`** to get verbose help on each command switch option.

FIGURE 6.1 Results from the GPResult utility



Applying LGPOs

As we discussed previously, policies that have been linked through Active Directory will take precedence over any established local group policies. Local group policies are typically applied to computers that are not part of a network or are in a network that does not have a domain controller, and thus do not use Active Directory.

Previous versions of Windows only contained one Local Group Policy Object that applied to all of the computer's users unless NTFS permissions were applied to the LGPO. However, Windows Vista changes that with the addition of Multiple Local Group Policy Objects (MLGPOs). Like Active Directory GPOs, MLGPOs are applied in a certain hierarchical order:

1. Local Computer Policy
2. Administrators and Non-Administrators Local Group Policy
3. User-Specific Group Policy

The Local Computer Policy is the only LGPO that includes computer and user settings; the other LGPOs only contain user settings. Settings applied here will apply to all users of the computer.

The Administrators and Non-Administrators LGPOs are new to Windows Vista. The Administrators LGPO is applied to users who are members of the built-in local Administrators group. As you might guess, the Non-Administrators LGPO is applied to users who are not members of the local Administrators group. Because each user of a computer can be classified as an administrator or a non-administrator either one policy or the other will apply.

User-Specific LGPOs are also new to Windows Vista. These LGPOs make it possible for specific policy settings to apply to a single user.

Like AD GPOs, any GPO settings applied lower in the hierarchy will override GPO settings applied higher in the hierarchy. For example, any user-specific GPO settings will override any conflicting administrator/non-administrator GPO settings or Local Computer Policy settings. And, of course, any AD GPO settings will still override any conflicting LGPO settings.

Domain administrators can disable LGPOs on Windows Vista computers by enabling the Turn Off Local Group Policy Objects Processing domain GPO setting, which you can find under `Computer Configuration\Administrative Templates\System\Group Policy`.

You apply an LGPO to a Windows Vista computer through the *Group Policy Object Editor snap-in* within the MMC. Figure 6.2 shows the Local Computer Policy for a Windows Vista computer.

In Exercise 6.1, you will see how to display the Local Computer Policy by adding the Group Policy Object Editor snap-in to the MMC.

EXERCISE 6.1

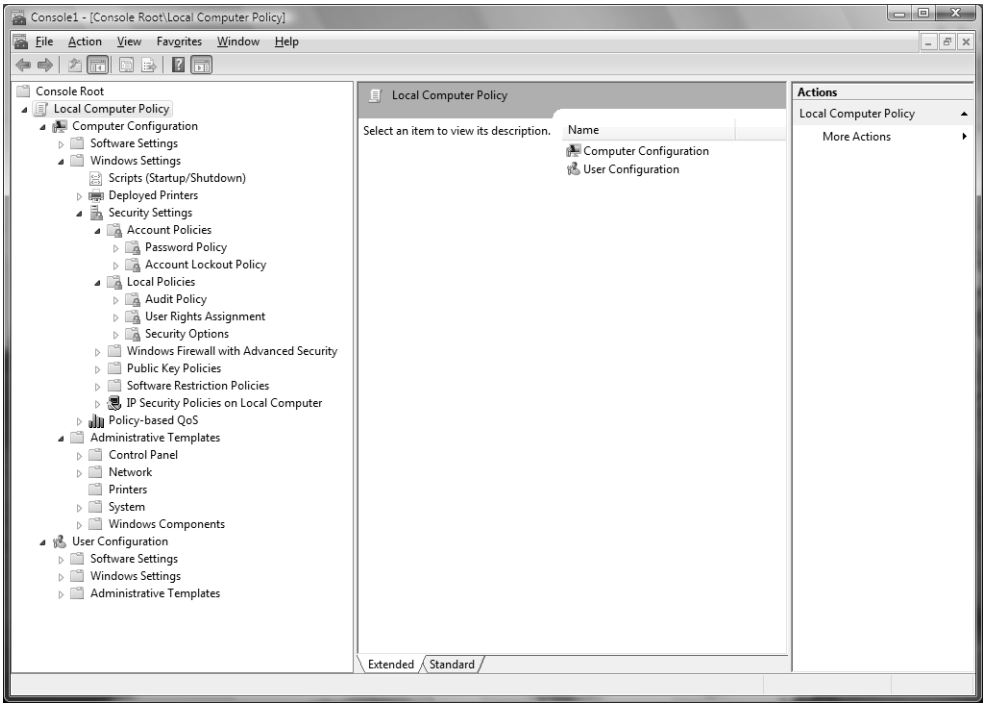
Adding the Local Computer Policy Snap-In to the MMC

1. Open the Admin Console MMC shortcut that was created in Exercise 5.1.
2. Select File ➢ Add/Remove Snap-in.
3. Highlight the Group Policy Object Editor Snap-in and click the Add button.

EXERCISE 6.1 *(continued)*

4. The Group Policy Object specifies Local Computer by default. Click the Finish button.
5. In the Add or Remove Snap-ins dialog box, click OK. Leave the Admin Console open, as it will be used for the other exercises in this chapter.

FIGURE 6.2 Local Computer Policy



In Exercise 6.2, you will see how to access the Administrators, Non-Administrators, and User-Specific LGPOs.

EXERCISE 6.2

Accessing the Administrators, Non-Administrators, and User-Specific LGPOs

1. For this exercise, we will start out with a new MMC. Select Start ➢ Run. In the Run dialog box, type **MMC** and press Enter.
2. Select File ➢ Add/Remove Snap-in.

EXERCISE 6.2 *(continued)*

3. Highlight the Group Policy Object Editor Snap-in and click the Add button.
4. Click Browse so that we can browse for a different GPO.
5. Click the Users tab.
6. Select the LGPO that you want to access and click OK.
7. In the Select Group Policy Object dialog box, click Finish.
8. In the Add or Remove Snap-ins dialog box, click OK. You may close the console when you are done looking at the LGPO settings.

Notice that the Administrators, Non-Administrators, and User-Specific LGPOs contain only User Configuration settings, not Computer Configuration settings.

Through the Local Computer Policy, you can set a wide range of security options under `Computer Configuration\Windows Settings\Security Settings`. This portion of the Local Computer Policy is also known as the Local Security Policy. The following sections describe in detail how to apply security settings through LGPOs. The two main areas of security configuration are as follows:

- Account policies, which are used to configure password and account lockout features
- Local policies, which are used to configure auditing, user rights, and security options

You can also access the Local Security Policy by running `secpol.msc` or by opening Control Panel and selecting Classic View ➢ Administrative Tools ➢ Local Security Policy.

You'll take a look at both the account policies and local policies in more detail in the following sections.

Using Account Policies

Account policies are used to specify the user account properties that relate to the logon process. They allow you to configure computer security settings for passwords and account lockout specifications.

If security is not an issue—perhaps because you are using your Windows Vista computer at home—then you don't need to bother with account policies. If, on the other hand, security

is important—for example, because your computer provides access to payroll information—then you should set very restrictive account policies.

Account policies at the LGPO level apply only to local user accounts, not domain accounts. To ensure that user account security is configured for domain user accounts, you must configure these policies at the Domain GPO level.

To access the Account Policies folder from the MMC, follow this path: Local Computer Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies. You will look at all these folders and how to use them throughout the rest of this chapter.

In the following sections you will learn about the password policies and account lockout policies that define how security is applied to account policies.

Setting Password Policies

Password policies ensure that security requirements are enforced on the computer. It is important to understand that the password policy is set on a per-computer basis; it cannot be configured for specific users. Figure 6.3 shows the password policies, which are described in Table 6.2.

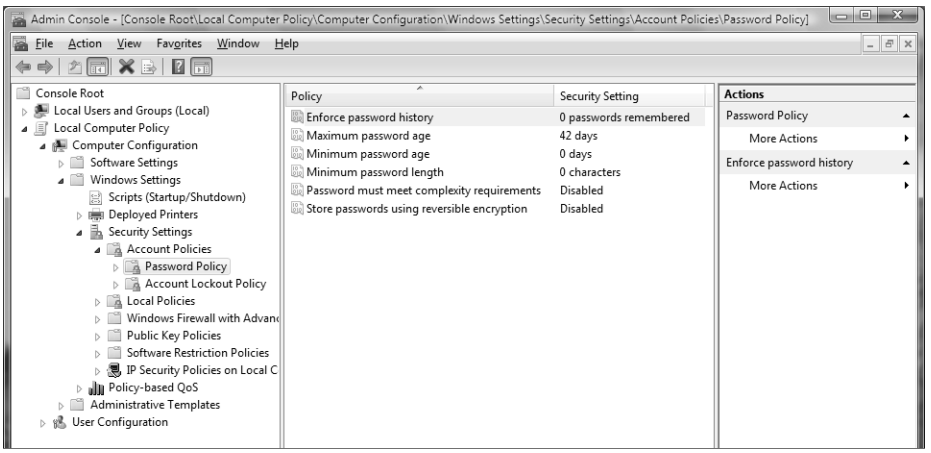
You can use the password policies in Table 6.2 as follows:

Enforce Password History Prevents users from repeatedly using the same passwords. Users must create a new password when their password expires or is changed.

Maximum Password Age Forces users to change their password after the maximum password age is exceeded. Setting this value to 0 will specify that the password will never expire.

Minimum Password Age Prevents users from changing their password several times in rapid succession in order to defeat the purpose of the Enforce Password History policy.

FIGURE 6.3 The password policies



Minimum Password Length Ensures that users create a password and specifies the length requirement for that password. If this option isn't set, users are not required to create a password at all.

Password Must Meet Complexity Requirements Passwords must be six characters or longer, and cannot contain the user's account name or any part of the user's full name. In addition, passwords must contain three of the following character types:

- English uppercase characters (*A* through *Z*)
- English lowercase characters (*a* through *z*)
- Decimal digits (0 through 9)
- Symbols (such as !, @, #, $, and %)

Store Passwords Using Reversible Encryption Provides a higher level of security for user passwords. This is required for Challenge Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS) and for Digest Authentication with Internet Information Services (IIS).

TABLE 6.2 Password Policy Options

Policy	Description	Default	Minimum	Maximum
Enforce Password History	Keeps track of user's password history	Remember 0 passwords	Same as default	Remember 24 passwords
Maximum Password Age	Determines maximum number of days user can keep valid password	Keep password for 42 days	Keep password for 1 day	Keep password for up to 999 days
Minimum Password Age	Specifies how long password must be kept before it can be changed	0 days (password can be changed immediately)	Same as default	998 days
Minimum Password Length	Specifies minimum number of characters password must contain	0 characters (no password required)	Same as default	14 characters
Password Must Meet Complexity Requirements	Requires that passwords meet minimum levels of complexity	Disabled		
Store Passwords Using Reversible Encryption	Specifies higher level of encryption for stored user passwords	Disabled		

In Exercise 6.3, you will configure password policies for your computer. This exercise assumes that you have added the Local Computer Policy snap-in to the MMC (see Exercise 6.1).

EXERCISE 6.3

Setting Password Policies

1. Open the Admin Console MMC shortcut that was configured in Exercise 6.1.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies ➢ Password Policy.
4. Open the Enforce Password History policy. On the Local Security Setting tab, specify that **5** passwords will be remembered. Click OK.
5. Open the Maximum Password Age policy. On the Local Security Setting tab, specify that the password expires in **60** days. Click OK.

Setting Account Lockout Policies

The *account lockout policies* specify how many invalid logon attempts should be tolerated. You configure the account lockout policies so that after *x* number of unsuccessful logon attempts within *y* number of minutes, the account will be locked for a specified amount of time or until the Administrator unlocks the account.

Account lockout policies are similar to a bank's arrangements for ATM access code security. You have a certain number of chances to enter the correct PIN. That way, anyone who steals your card can't just keep guessing your access code until they get it right. Typically, after three unsuccessful attempts, the ATM takes the card. Then you need to request a new card from the bank.

Figure 6.4 shows the account lockout policies, which are described in Table 6.3.

The Account Lockout Duration and Reset Account Lockout Counter After policies will be disabled until a value is specified for the Account Lockout Threshold. After the Account Lockout Threshold is set, the Account Lockout Duration and Reset Account Lockout Counter After policies will be set to 30 minutes. If you set the Account Lockout Duration to 0, then the account will remain locked out until an administrator unlocks it.

The Reset Account Lockout Counter After value must be equal to or less than the Account Lockout Duration value.

FIGURE 6.4 The account lockout policies

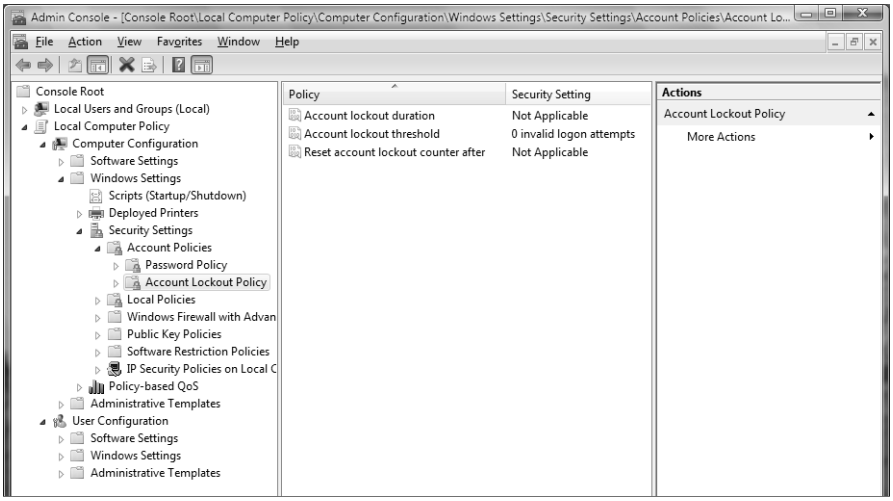


TABLE 6.3 Account Lockout Policy Options

Policy	Description	Default	Minimum	Maximum
Account Lockout Duration	Specifies how long account will remain locked if Account Lockout Threshold is reached	Disabled, but if Account Lockout Threshold is enabled, 30 minutes	Same as default	99,999 minutes
Account Lockout Threshold	Specifies number of invalid attempts allowed before account is locked out	0 (disabled; account will not be locked out)	Same as default	999 attempts
Reset Account Lockout Counter After	Specifies how long counter will remember unsuccessful logon attempts	Disabled, but if Account Lockout Threshold is enabled, 30 minutes	Same as default	99,999 minutes

In Exercise 6.4, you will configure account lockout policies and test their effects. This exercise assumes that you have completed all of the previous exercises in this chapter.

EXERCISE 6.4

Setting Account Lockout Policies

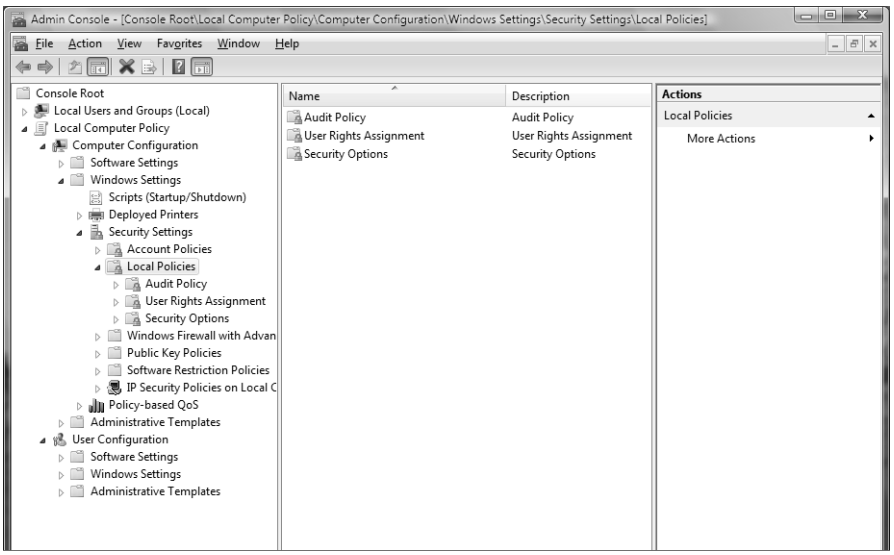
1. Open the Admin Console MMC shortcut that was configured in Exercise 6.1.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies ➢ Account Lockout Policy.
4. Open the Account Lockout Threshold policy. On the Local Security Setting tab, specify that the account will lock after **3** invalid logon attempts. Click OK.
5. Accept the Suggested Value Changes for the Account Lockout Duration and Reset Account Lockout Counter After policies by clicking OK.
6. Open the Account Lockout Duration policy. On the Local Security Setting tab, specify that the account will remain locked for **5** minutes. Click OK.
7. Accept the Suggested Value Changes for the Reset Account Lockout Counter After policy by clicking OK.
8. Log off your administrator account. Try to log on as Emily with an incorrect password four times.
9. After you see the error message stating that the referenced account has been locked out, log on as an administrator.
10. To unlock Emily's account, open the Local Users and Groups snap-in in the MMC, expand the Users folder, and double-click user Emily.
11. On the General tab of Emily's Properties dialog box, click to remove the check from the Account Is Locked Out check box. Then click OK.

Using Local Policies

As you learned in the preceding section, account policies are used to control logon procedures. When you want to control what a user or group can do *after* logging on, you use *local policies*. With local policies, you can implement auditing, specify user rights, and set security options.

To use local policies, first add the Local Computer Policy snap-in to the MMC (see Exercise 6.1). Then, from the MMC, follow this path to access the Local Policies folders: Local Computer Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies. Figure 6.5 shows the three Local Policies folders: `Audit Policy`, `User Rights Assignment`, and `Security Options`. You will look at each of those in the following sections.

FIGURE 6.5 Accessing the Local Policies folders



Setting Audit Policies

Audit policies can be implemented to track success or failure of specified user actions. You audit events that pertain to user management through the audit policies. By tracking certain events, you can create a history of specific tasks, such as user creation and successful or unsuccessful logon attempts. You can also identify security violations that arise when users attempt to access system management tasks for which they do not have permission.

Users who try to go to areas for which they do not have permission usually fall into two categories: hackers and people who are just curious to see what they can get away with. Both are very dangerous.

When you define an audit policy, you can choose to audit success or failure of specific events. The success of an event means that the task was successfully accomplished. The failure of an event means that the task was not successfully accomplished.

By default, auditing is not enabled, and it must be manually configured. Once auditing has been configured, you can see the results of the audit in the Security log using the Event Viewer utility. (We cover the Event Viewer utility in Chapter 11, "Maintaining and Optimizing Windows Vista.")

Auditing too many events can degrade system performance due to its high processing requirements. Auditing can also use excessive disk space to store the audit log. You should use this utility judiciously.

Figure 6.6 shows the audit policies, which are described in Table 6.4.

FIGURE 6.6 The audit policies

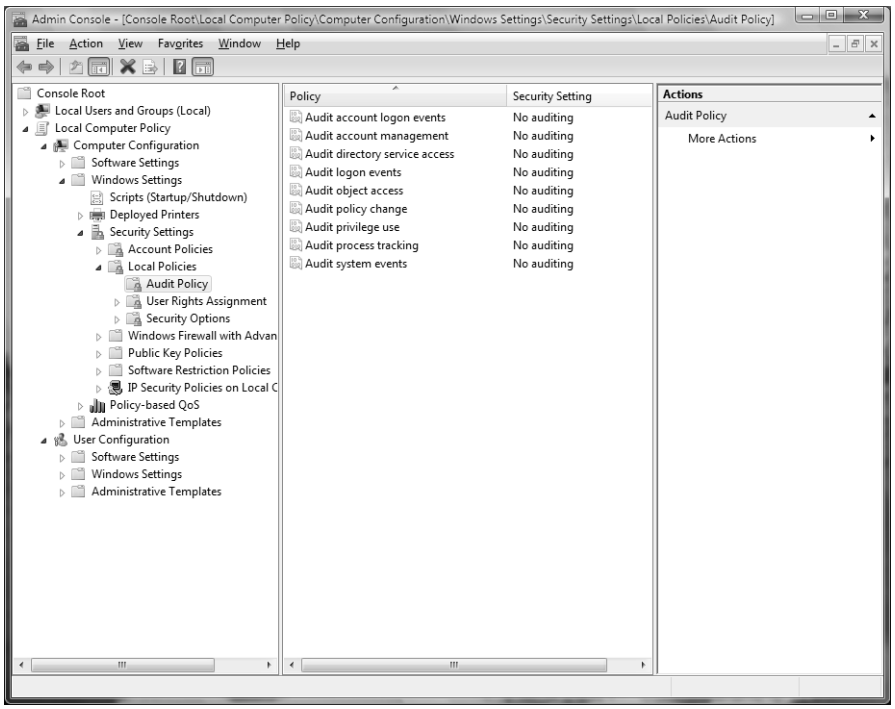


TABLE 6.4 Audit Policy Options

Policy	Description
Audit Account Logon Events	Tracks when a user logs on, logs off, or makes a network connection
Audit Account Management	Tracks user and group account creation, deletion, and management actions, such as password changes

TABLE 6.4 Audit Policy Options *(continued)*

Policy	Description
Audit Directory Service Access	Tracks directory service accesses
Audit Logon Events	Audits events related to logon, such as running a logon script or accessing a roaming profile
Audit Object Access	Enables auditing of access to files, folders, and printers
Audit Policy Change	Tracks any changes to the audit policies, trust policies, or user rights assignment policies
Audit Privilege Use	Tracks users exercising a user right
Audit Process Tracking	Tracks events such as activating a program, accessing an object, and exiting a process
Audit System Events	Tracks system events such as shutting down or restarting the computer, as well as events that relate to the Security log in Event Viewer

After you set the Audit Object Access policy to enable auditing of object access, you must enable file auditing through NTFS security or print auditing through printer security.

In Exercise 6.5, you will configure audit policies and view their results. This exercise assumes that you have completed all previous exercises in this chapter.

EXERCISE 6.5

Setting Audit Policies

1. Open the Admin Console MMC shortcut that you configured in Exercise 6.1.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Audit Policy.
4. Open the Audit Account Logon Events policy. Check the boxes for Success and Failure. Click OK.

EXERCISE 6.5 *(continued)*

5. Open the Audit Account Management policy. Check the boxes for Success and Failure. Click OK.
6. Log off your administrator account. Attempt to log back on as your administrator account with an incorrect password. The logon should fail (because the password is incorrect).
7. Log on as an administrator.
8. Select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Event Viewer to open Event Viewer.
9. From Event Viewer, open the Security log by selecting Windows Logs ➢ Security. You should see the audited events listed with a Task Category of Credential Validation.

You may want to limit the number of events that are audited. If you audit excessive events on a busy computer, the log file can grow very quickly. In the event that the log file becomes full, you can configure the computer to shut down through a security option policy, Audit: Shut Down System Immediately if Unable to Log Security Audits. If this option is triggered, the only user who will be able to log on to the computer will be an administrator until the log is cleared. If this option is not enabled and the log file becomes full, you will have the option of overwriting older log events. Setting security option policies is covered later in this chapter, in the section "Defining Security Options."

Assigning User Rights

The *user right policies* determine what rights a user or group has on the computer. User rights apply to the system. They are not the same as permissions, which apply to a specific object (permissions are discussed later in this chapter, in "Managing File and Folder Security").

An example of a user right is the Back Up Files and Directories right. This right allows a user to back up files and folders, even if the user does not have permissions that have been defined through NTFS file system permissions. The other user rights are similar because they deal with system access as opposed to resource access.

Figure 6.7 shows the user right policies, which are described in Table 6.5. The five user rights marked with an asterisk (*) are new in Windows Vista.

FIGURE 6.7 The user right policies

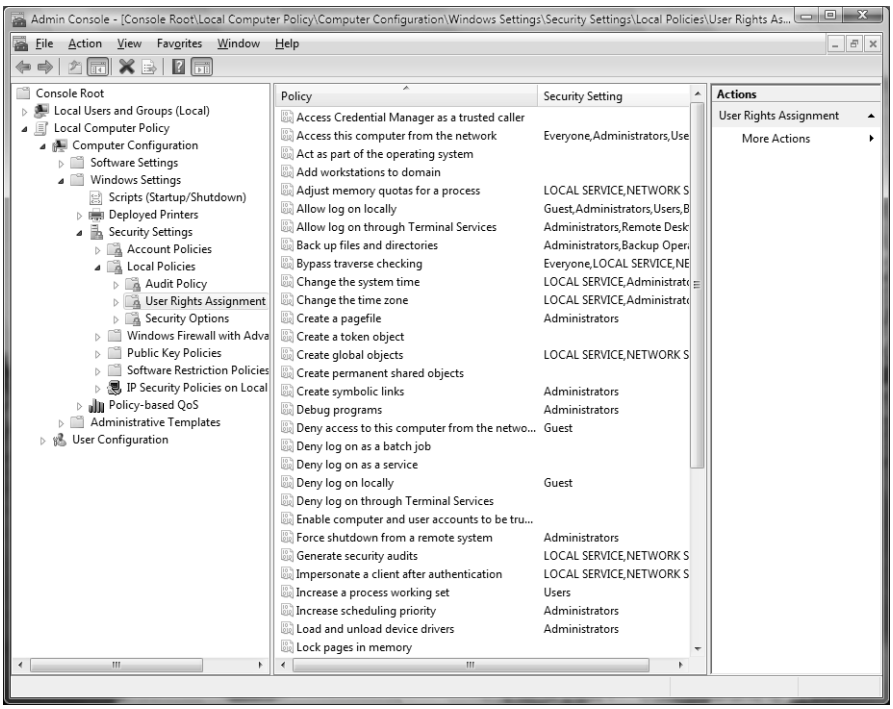


TABLE 6.5 User Rights Assignment Policy Options

Right	Description
* Access Credential Manager as a Trusted Caller	Used to back up and restore Credential Manager.
Access This Computer from the Network	Allows a user to access the computer from the network.
Act as Part of the Operating System	Allows low-level authentication services to authenticate as any user.
Add Workstations to Domain	Allows a user to create a computer account on the domain.

TABLE 6.5 User Rights Assignment Policy Options *(continued)*

Right	Description
Adjust Memory Quotas for a Process	Allows you to configure how much memory can be used by a specific process.
Allow Log on Locally	Allows a user to log on at the physical computer.
Allow Log on through Terminal Services	Gives a user permission to log on through Terminal Services. Does not affect Windows 2000 computers prior to SP2.
Back Up Files and Directories	Allows a user to back up all files and directories, regardless of how the file and directory permissions have been set.
Bypass Traverse Checking	Allows a user to pass through and traverse the directory structure, even if that user does not have permissions to list the contents of the directory.
Change the System Time	Allows a user to change the internal time and date on the computer.
* Change the Time Zone	Allows a user to change the time zone.
Create a Pagefile	Allows a user to create or change the size of a page file.
Create a Token Object	Allows a process to create a token if the process uses an internal API to create the token.
Create Global Objects	Allows a user to create global objects when connected using Terminal Server.
Create Permanent Shared Objects	Allows a process to create directory objects through the Object Manager.
* Create Symbolic Links	Allows a user to create a symbolic link.
Debug Programs	Allows a user to attach a debugging program to any process.
Deny Access to This Computer from the Network	Allows you to deny specific users or groups access to this computer from the network. Overrides the Access This Computer from the Network policy for accounts present in both policies.

TABLE 6.5 User Rights Assignment Policy Options *(continued)*

Right	Description
Deny Log on as a Batch Job	Allows you to prevent specific users or groups from logging on as a batch file. Overrides the Log On as a Batch Job policy for accounts present in both policies.
Deny Log on as a Service	Allows you to prevent specific users or groups from logging on as a service. Overrides the Log On as a Service policy for accounts present in both policies.
Deny Log on Locally	Allows you to deny specific users or groups access to the computer locally. Overrides the Log On Locally policy for accounts present in both policies.
Deny Log on through Terminal Services	Specifies that a user is not able to log on through Terminal Services. Does not affect Windows 2000 computers prior to SP2.
Enable Computer and User Accounts to Be Trusted for Delegation	Allows a user or group to set the Trusted for Delegation setting for a user or computer object.
Force Shutdown from a Remote System	Allows the system to be shut down by a user at a remote location on the network.
Generate Security Audits	Allows a user, group, or process to make entries in the Security log.
Impersonate a Client After Authentication	Enables programs running on behalf of a user to impersonate a client.
* Increase a Process Working Set	Allows the size of a process working set to be increased.
Increase Scheduling Priority	Specifies that a process can increase or decrease the priority that is assigned to another process.
Load and Unload Device Drivers	Allows a user to dynamically unload and load device drivers. This right does not apply to Plug and Play drivers.
Lock Pages in Memory	Allows an account to create a process that runs only in physical RAM, preventing it from being paged.

TABLE 6.5 User Rights Assignment Policy Options *(continued)*

Right	Description
Log On as a Batch Job	Allows a process to log on to the system and run a file that contains one or more operating system commands.
Log On as a Service	Allows a service to log on in order to run the specific service.
Manage Auditing and Security Log	Allows a user to enable object access auditing for files and other Active Directory objects. This right does not allow a user to enable general object access auditing in the Local Security Policy.
* Modify an Object Label	Allows a user to change the integrity level of files, folders, or other objects.
Modify Firmware Environment Variables	Allows a user to install or upgrade Windows. It also allows a user or process to modify the firmware environment variables stored in NVRAM of non-x86-based computers. This right does *not* affect the modification of system environment variables or user environment variables.
Perform Volume Maintenance Tasks	Allows a user to perform volume maintenance tasks such as defragmentation and error checking.
Profile Single Process	Allows a user to monitor nonsystem processes through performance-monitoring tools.
Profile System Performance	Allows a user to monitor system processes through performance-monitoring tools.
Remove Computer from Docking Station	Allows a user to undock a laptop through the Windows Vista user interface.
Replace a Process Level Token	Allows a process, such as Task Scheduler, to call an API to start another service.
Restore Files and Directories	Allows a user to restore files and directories, regardless of file and directory permissions.
Shut Down the System	Allows a user to shut down the Windows Vista computer locally.

TABLE 6.5 User Rights Assignment Policy Options *(continued)*

Right	Description
Synchronize Directory Service Data	Allows a user to synchronize Active Directory data.
Take Ownership of Files or Other Objects	Allows a user to take ownership of system objects, such as files, folders, printers, and processes.

In Exercise 6.6, you will apply a user right policy. This exercise assumes that you have completed all of the previous exercises in this chapter.

EXERCISE 6.6

Setting User Rights

1. Open the Admin Console MMC shortcut that was configured in Exercise 6.1.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ User Rights Assignment.
4. Open the Log On as a Service user right.
5. Click the Add User or Group button. The Select Users or Groups dialog box appears.
6. Click the Advanced button, and then select Find Now.
7. Select user Emily. Click OK.
8. Click OK in the Select Users or Groups dialog box.
9. In the Log On as a Service Properties dialog box, click OK.

Defining Security Options

Security option policies are used to configure security for the computer. Unlike user right policies, which are applied to a user or group, security option policies apply to the computer. Figure 6.8 shows the security option policies, which are described briefly in Table 6.6. The options marked with an asterisk are new to Windows Vista, and the default settings marked with an asterisk have changed in Windows Vista.

FIGURE 6.8 The security option policies

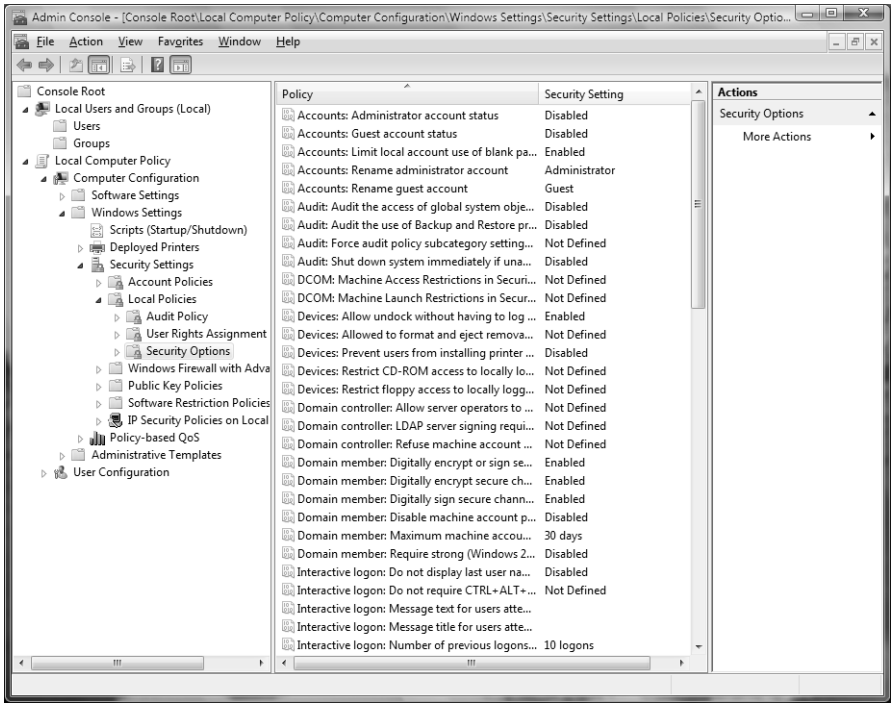


TABLE 6.6 Security Options

Option	Description	Default
Accounts: Administrator Account Status	Specifies whether the Administrator account is enabled or disabled under normal operation. Booting under Safe Mode, the Administrator account is enabled, regardless of this setting.	* Disabled
Accounts: Guest Account Status	Determines whether the Guest account is enabled or disabled.	Disabled
Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only	Determines whether a local user with a blank password will be able to log on remotely. If this policy is enabled, users with blank passwords will only be able to log on locally. This setting does not apply to domain logon accounts.	Enabled

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Accounts: Rename Administrator Account	Allows the Administrator account to be renamed.	Administrator account is named Administrator.
Accounts: Rename Guest Account	Allows the Guest account to be renamed.	Guest account is named Guest.
Audit: Audit the Access of Global System Objects	Allows access of global system objects to be audited.	Disabled
Audit: Audit the Use of Backup and Restore Privilege	Allows the use of backup and restore privileges to be audited.	Disabled
* Audit: Force Audit Policy Subcategory Settings (Windows Vista or later) to Override Audit Policy Category Settings	Allows audit policy subcategory settings to override audit policy category settings at the category level.	Not defined
Audit: Shut Down System Immediately if Unable to Log Security Audits	Specifies that the system shuts down immediately if it is unable to log security audits.	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) Syntax	Specifies the users who can access DCOM applications.	Not defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) Syntax	Specifies the users who can launch DCOM applications.	Not defined
Devices: Allow Undock Without Having to Log On	Allows a user to undock a laptop computer from a docking station by pushing the computer's eject button without first having to log on.	Enabled
Devices: Allowed to Format and Eject Removable Media	Specifies which users can format and eject removable NTFS media.	* Not defined

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Devices: Prevent Users from Installing Printer Drivers	If enabled, allows only Administrators to install print drivers for a network printer.	Disabled
Devices: Restrict CD-ROM Access to Locally Logged-On User Only	Specifies whether the CD-ROM is accessible to local users and network users. If enabled, only the local user can access the CD-ROM, but if no local user is logged in, then the CD-ROM can be accessed over the network. If disabled or not defined, then access is not restricted.	* Not defined
Devices: Restrict Floppy Access to Locally Logged-On User Only	Specifies whether the floppy drive is accessible to local users and network users. If enabled, only the local user can access the floppy, but if no local user is logged in, then the floppy can be accessed over the network. If disabled or not defined, then access is not restricted.	* Not defined
Domain Controller: Allow Server Operators to Schedule Tasks	Allows server operators to schedule specific tasks to occur at specific times or intervals. Applies only to tasks scheduled through the AT command and does not affect tasks scheduled through Task Scheduler.	Not defined
Domain Controller: LDAP Server Signing Requirements	Specifies whether a Lightweight Directory Access Protocol server requires server signing with an LDAP client.	Not defined
Domain Controller: Refuse Machine Account Password Changes	Specifies whether a domain controller will accept password changes for computer accounts.	* Not defined
Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	Specifies whether a secure channel must be created with the domain controller before secure channel traffic is generated.	Enabled
Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Specifies that if a secure channel can be created between the domain controller and the domain controller partner, it will be.	Enabled

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Domain Member: Digitally Sign Secure Channel Data (When Possible)	Specifies that all secure channel traffic be signed if both domain controller partners who are transferring data are capable of signing secure data.	Enabled
Domain Member: Disable Machine Account Password Changes	Specifies whether a domain member must periodically change its computer account password as defined in the Domain Member: Maximum Machine Account Password Age setting.	Disabled
Domain Member: Maximum Machine Account Password Age	Specifies the maximum age of a computer account password.	30 days
Domain Member: Require Strong (Windows 2000 or Later) Session Key	If enabled, the domain controller must encrypt data with a 128-bit session key; if not enabled, 64-bit session keys can be used.	Disabled
Interactive Logon: Do Not Display Last User Name	Prevents the last username in the logon screen from being displayed.	Disabled
Interactive Logon: Do Not Require Ctrl+Alt+Del	Allows the Ctrl+Alt+Del requirement for logon to be disabled.	Not defined, but it is automatically used on standalone workstations, meaning users who log on to the workstation see a start screen with icons for all users who have been created on the computer.
Interactive Logon: Message Text for Users Attempting to Log On	Displays message text for users trying to log on, usually configured for displaying legal text messages.	Not defined
Interactive Logon: Message Title for Users Attempting to Log On	Displays a message title for users trying to log on.	Not defined

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Interactive Logon: Number of Previous Logon Attempts to Cache (in Case Domain Controller Is Not Available)	Specifies the number of previous logon attempts stored in the cache. This option is useful if a domain controller is not available.	10
Interactive Logon: Prompt User to Change Password Before Expiration	Prompts the user to change the password before expiration.	14 days before password expiration
Interactive Logon: Require Domain Controller Authentication to Unlock	Specifies that a user name and password be required to unlock a locked computer. When this is disabled, a user can unlock a computer with cached credentials. When this is enabled, a user is required to authenticate to a domain controller to unlock the computer.	Disabled
* Interactive Logon: Require Smart Card	Specifies that a smart card is required to log on to the computer.	Disabled
Interactive Logon: Smart Card Removal Behavior	Specifies what happens if a user who is logged on with a smart card removes the smart card.	No action
Microsoft Network Client: Digitally Sign Communications (Always)	Specifies that the server should always digitally sign client communication.	Disabled
Microsoft Network Client: Digitally Sign Communications (if Server Agrees)	Specifies that the server should digitally sign client communication when possible.	Enabled
Microsoft Network Client: Send Unencrypted Password to Third-Party SMB Servers	Allows third-party Server Message Block servers to use unencrypted passwords for authentication.	Disabled
Microsoft Network Client: Amount of Idle Time Required: Before Suspending Session	Allows sessions to be disconnected when they are idle.	* 15 minutes

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Microsoft Network Server: Digitally Sign Communications (Always)	Ensures that server communications will always be digitally signed.	Disabled
Microsoft Network Server: Digitally Sign Communications (if Client Agrees)	Specifies that server communications should be signed when possible.	Disabled
Microsoft Network Server: Disconnect Clients when Logon Hours Expire	If a user logs on and then their logon hours expire, specifies whether an existing connection will remain connected or be disconnected.	* Enabled
Network Access: Allow Anonymous SID/Name Translation	Specifies whether an anonymous user can request the security identifier (SID) attributes for another user.	Disabled
Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts	If enabled, prevents an anonymous connection from enumerating Security Account Manager (SAM) accounts.	Enabled
Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts and Shares	If enabled, prevents an anonymous connection from enumerating Security Account Manager (SAM) accounts and network shares.	Disabled
* Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication	Specifies whether passwords, credentials, and .NET Passports are stored and available for use after a user is authenticated to a domain.	Disabled
Network Access: Let Everyone Permissions Apply to Anonymous Users	Specifies whether Everyone permission will apply to anonymous users.	Disabled
Network Access: Named Pipes that Can Be Accessed Anonymously	Specifies which communication sessions are allowed to anonymous users.	Defined

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Network Access: Remotely Accessible Registry Paths	Determines which Registry paths will be accessible when the winreg key is accessed for remote Registry access, regardless of the ACL setting.	Defined
* Network Access: Remotely Accessible Registry Paths and Sub-Paths	Determines which Registry paths and subpaths will be accessible when the winreg key is accessed for remote Registry access, regardless of the ACL setting.	Defined
* Network Access: Restrict Anonymous Access to Named Pipes and Shares	Specifies whether anonymous access is allowed to shares and pipes for the Network Access: Named Pipes that Can Be Accessed Anonymously and Network Access: Shares That Can Be Accessed Anonymously policies	Enabled
Network Access: Shares That Can Be Accessed Anonymously	Specifies which network shares can be accessed by anonymous users.	* Not defined
Network Access: Sharing and Security Model for Local Accounts	Specifies how local accounts will be authenticated over the network.	* Classic – Local Users Authenticate as Themselves
Network Security: Do Not Store LAN Manager Hash Value on Next Password Change	Specifies whether LAN Manager will store hash values from password changes.	* Enabled
Network Security: Force Logoff when Logon Hours Expire	Specifies whether a user with a current connection will be automatically logged off when the user's logon hours expire.	Disabled
Network Security: LAN Manager Authentication Level	Specifies the LAN Manager Authentication Level.	* Send NTLMv2 Response Only
Network Security: LDAP Client Signing Requirements	Specifies the client signing requirements that will be enforced for LDAP clients.	Negotiate signing

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Clients	Specifies the minimum security standards for application-to-application client communications.	No minimum
Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Servers	Specifies the minimum security standards for application-to-application server communications.	No minimum
Recovery Console: Allow Automatic Administrative Logon	Specifies whether a password is required for Administrative logon when the Recovery Console is loaded. If Enabled, the password is not required.	Disabled
Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders	Allows you to copy files from all drives and folders when the Recovery Console is loaded.	Disabled
Shutdown: Allow System to Be Shut Down Without Having to Log On	Allows the user to shut down the system without logging on.	Enabled
Shutdown: Clear Virtual Memory Pagefile	Specifies whether the virtual memory pagefile will be cleared when the system is shut down.	Disabled
* System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer	Specifies whether a password is required to use a private key.	Not defined
System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing and Signing	Specifies which encryption algorithms should be supported for encrypting, hashing, and signing file data.	Disabled

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
System Objects: Default Owner for Objects Created by Members of the Administrators Group	Determines whether, when an object is created by a member of the Administrators group, the owner will be the Administrators group or user who created the object.	Object creator
System Objects: Require Case Insensitivity for Non-Windows Subsystems	By default, Windows Vista does not specify case insensitivity for file subsystems. However, subsystems such as POSIX use case-sensitive file systems, so this option allows you to configure case sensitivity.	Enabled
System Objects: Strengthen Default Permissions of Internal System Objects (e.g., Symbolic Links)	Specifies the default discretionary access control list for objects.	Enabled
* System Settings: Optional Subsystems	Specifies the subsystems that are used to support applications in your environment.	POSIX
* System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Specifies whether digital certificates are required when a user or process runs an EXE file.	Disabled
* User Account Control: Admin Approval Mode for the Built-in Administrator Account	If Enabled, the built-in Administrator account will require approval for any operation that requires privilege elevation. If Disabled, the built-in Administrator account will use XP-compatible mode with full administrative privileges.	Disabled
* User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode	Specifies the method for approval of privilege elevation for administrators.	Prompt for Consent

TABLE 6.6 Security Options *(continued)*

Option	Description	Default
* User Account Control: Behavior of the Elevation Prompt for Standard Users	Specifies the method for approval of privilege elevation for standard users.	Prompt for Credentials
* User Account Control: Detect Application Installations and Prompt for Elevation	Specifies how applications are installed and whether approval is required.	Enabled
* User Account Control: Only Elevate Executables that are Signed and Validated	Specifies whether PKI signature checks are required for applications that request privilege elevation.	Disabled
* User Account Control: Only Elevate UIAccess Applications that are Installed in Secure Locations	Requires that applications executing with a UIAccess integrity level reside in a secure file system location.	Enabled
* User Account Control: Run All Administrators in Admin Approval Mode	Enforces UAC policy for all users, including administrators.	Enabled
* User Account Control: Switch to the Secure Desktop When Prompting for Elevation	If Enabled, elevation requests will go to the Secure Desktop. If Disabled, elevation requests will appear on the users' desktop.	Enabled
* User Account Control: Virtualize File and Registry Write Failures to Per-User Locations	Allows standard users to run pre-Windows Vista applications that formerly required administrator-level access to write to protected locations.	Enabled

In Exercise 6.7, you will define some security option policies and see how they work. This exercise assumes that you have completed all of the previous exercises in this chapter.

EXERCISE 6.7

Defining Security Options

1. Open the Admin Console MMC shortcut that was configured in Exercise 6.1.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options.
4. Open the policy Interactive Logon: Message Text for Users Attempting to Log On. On the Local Policy Setting tab, type **Welcome to all authorized users**. Click OK.
5. Open the policy Interactive Logon: Message Title for Users Attempting to Log On. On the Local Security Setting tab, type **Welcome Message**. Click OK.
6. Open the policy Interactive Logon: Prompt User to Change Password before Expiration. On the Local Security Setting tab, type **3** days. Click OK.
7. Log off your administrator account and see the Welcome Message text appear. Click OK.
8. Log on as an administrator.

User Account Control

Most administrators have had to wrestle with the balance between security and enabling applications to run correctly. In the past, some applications simply would not run correctly under Windows unless the user running the application was a local administrator. Unfortunately, granting local administrator permissions to a user also allows the user to install software and hardware, change configuration settings, modify local user accounts, and delete critical files. Even more troubling is the fact that malware that infects a computer while an administrator is logged in is also able to perform those same functions.

Limited user accounts in Windows XP were supposed to allow applications to run correctly and allow users to perform necessary tasks. However, in practical application, it did not work as advertised. Many applications require that users have permissions to write to protected folders and to the Registry, and limited user accounts did not allow users to do so.

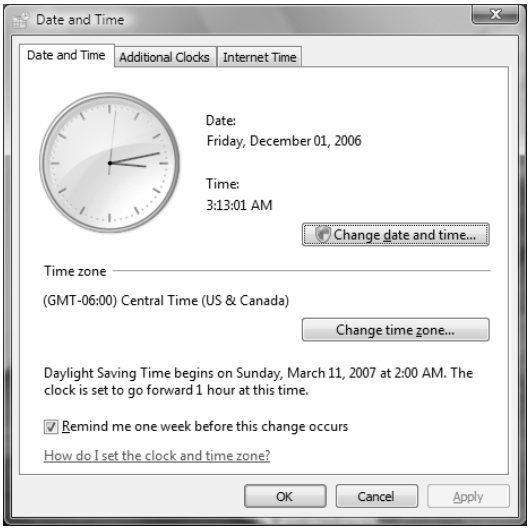
Windows Vista's answer to the problem is User Account Control (UAC). UAC enables non-administrator users to perform standard tasks, such as install a printer, configure a VPN or wireless connection, and install updates, while preventing them from performing tasks that require administrative privileges, such as installing applications.

Privilege Elevation

UAC protects computers by requiring privilege elevation for all users, even users who are members of the local Administrators group. As you have no doubt seen by now, UAC will prompt you for permission when performing a task that requires privilege elevation. This prevents malware from silently launching processes without your knowledge.

Privilege elevation is required for any feature that contains the four-color security shield. For example, the small shield shown on the Change Date and Time button in the Date and Time dialog box in Figure 6.9 indicates an action that requires privilege elevation.

FIGURE 6.9 Date and Time dialog box



Elevated Privileges for Users

By default, local administrators are logged on as standard users. When administrators attempt to perform a task that requires privilege escalation, they are prompted for confirmation by default. You can require administrators to authenticate when performing a task that requires privilege escalation by changing the User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode policy setting to Prompt for Credentials. On the other hand, if you don't want UAC to prompt administrators for confirmation when elevating privileges, you can change the policy setting to Elevate Without Prompting.

Non-administrator accounts are called standard users. When standard users attempt to perform a task that requires privilege elevation, they are prompted for a password of a user account that has administrative privileges. You cannot configure UAC to automatically allow

standard users to perform administrative tasks, nor can you configure UAC to prompt a standard user for confirmation before performing administrative tasks. If you do not want standard users to be prompted for credentials when attempting to perform administrative tasks, you can automatically deny elevation requests by changing the User Account Control: Behavior of the Elevation Prompt for Standard Users policy setting to Automatically Deny Elevation Requests.

The built-in Administrator account, though disabled by default, is not affected by UAC. UAC will not prompt the Administrator account for elevation of privileges. Thus, it is important to use a normal user account whenever possible, and use the built-in Administrator account only when absolutely necessary.

Group policy settings can affect how UAC prompts for privilege elevation. Be sure to review the new security options relating to UAC in the "Defining Security Options" section earlier in this chapter.

In Exercise 6.8, you will see how UAC affects administrator and non-administrator accounts differently. This exercise assumes that you have completed all of the previous exercises in this chapter.

EXERCISE 6.8

Using Privilege Elevation in User Account Control

1. Select Start ➢ Control Panel ➢ Security ➢ Windows Firewall.
2. Click Turn Windows Firewall On or Off. The UAC box should prompt you for permission to continue. Click Continue. You should be allowed access to the Windows Firewall Settings dialog box.
3. Log off your administrator account and log on as Emily, who is configured as a standard user account.
4. Select Start ➢ Control Panel ➢ Security ➢ Windows Firewall.
5. Click Turn Windows Firewall On or Off. The UAC box should prompt you for an administrator's credentials.
6. Click one of the administrator-level accounts, type the appropriate password, and click OK. You should be allowed access to the Windows Firewall Settings dialog box.
7. Log off as Emily and log on as an administrator.

Elevated Privileges for Executables

You can also enable an executable file to run with elevated privileges. To do so, on a one-time basis, you can right click on a shortcut or executable and select Run as Administrator.

But what if you need to configure an application to always run with elevated privileges for a user? To do so, log in as an administrator, right-click on a shortcut or executable, and select Properties. On the Compatibility tab, check the Run This Program as an Administrator check box. If the Run This Program as an Administrator check box is unavailable, the program is blocked from permanently running as an administrator, the program doesn't need administrative privileges, or you are not logged on as an administrator.

Registry and File Virtualization

Windows Vista uses a feature called Registry and file virtualization to enable non-administrator users to run applications that previously required administrative privileges to run correctly. As discussed earlier, some applications write to the Registry and to protected folders, such as `C:\Windows` and `C:\Program Files`. For non-administrator users, Windows Vista redirects any attempts to write to protected locations to a per-user location. By doing so, Windows Vista enables users to use the application successfully while it protects critical areas of the system.

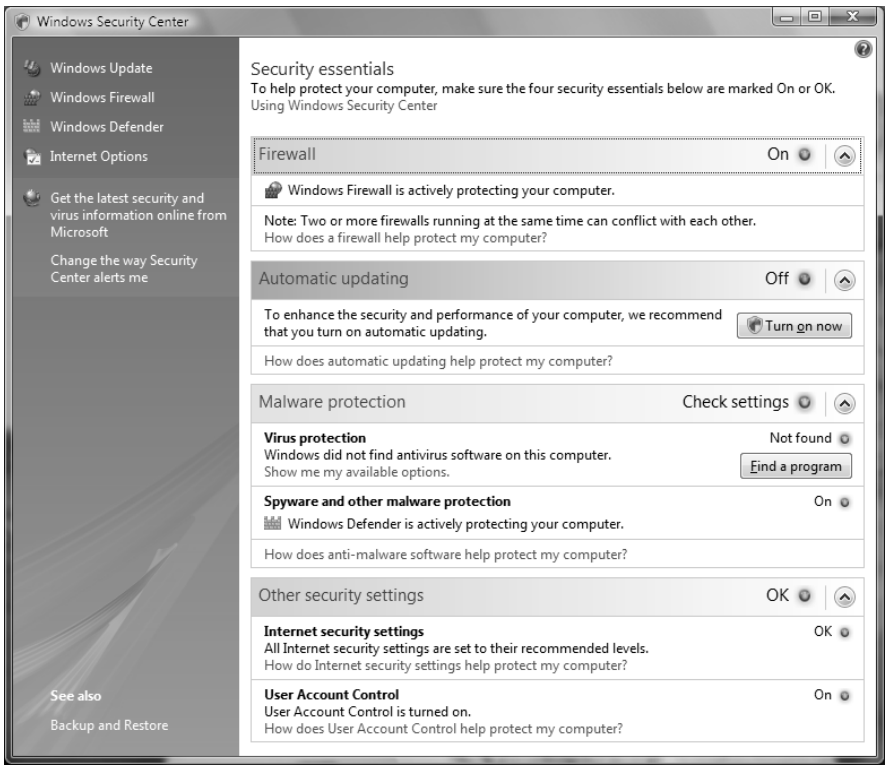
Using Windows Security Center

Windows Security Center, shown in Figure 6.10, is designed to allow you to monitor and configure critical settings through a centralized dialog box. Critical settings include Firewall, Automatic Updating, Malware Protection, and Other Security Settings. Malware Protection includes virus protection (not included with Windows Vista) and spyware protection (included through Windows Defender). The Other Security Settings category includes Internet Security Settings and User Account Control.

Windows Security Center lists whether each security feature is enabled and whether the security feature is up-to-date. If the feature is not up-to-date, Windows Security Center will make recommendations as to what action will make your computer more secure. In addition to managing security options through the Windows Security Center, you can manage all of the security options in an enterprise environment through Active Directory.

Automatic Update is covered in greater detail in Chapter 1, "Getting Started with Windows Vista." Internet Explorer Security options are covered in greater detail in Chapter 9, "Configuring Internet Explorer." User Account Control, Windows Firewall, and Windows Defender are covered in greater detail in this chapter.

FIGURE 6.10 Windows Security Center



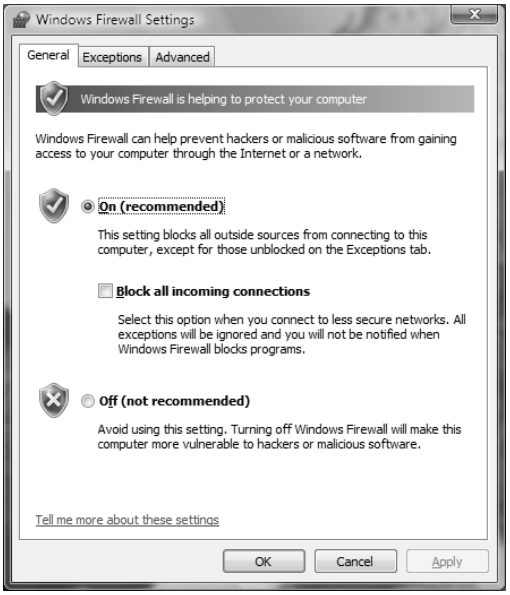
Using Windows Firewall

Windows Firewall, which is included with Windows Vista, helps to prevent unauthorized users or malicious software from accessing your computer. Windows Firewall does not allow unsolicited traffic (traffic that was not sent in response to a request) to pass through the firewall.

You configure Windows Firewall by selecting Start ➢ Control Panel ➢ Classic View ➢ Windows Firewall, then clicking Change Settings. The Windows Firewall Settings dialog box will appear, as shown in Figure 6.11.

Privilege escalation is required to make changes to Windows Firewall.

FIGURE 6.11 Windows Firewall Settings dialog box



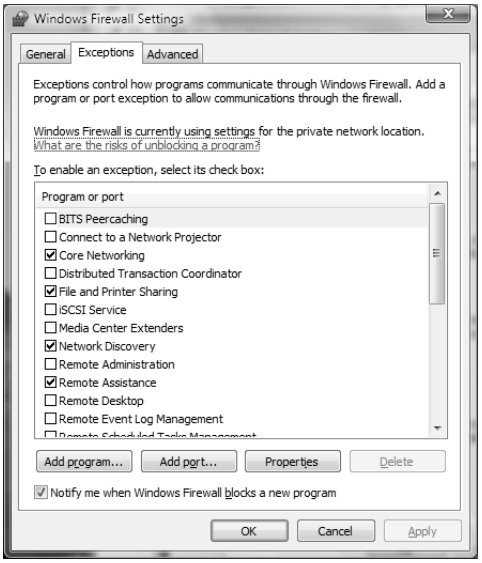
The General tab of the Windows Firewall Settings dialog box allows you to turn Windows Firewall on or off. The On setting will block external sources except those that are specified on the Exceptions tab. The Off setting will allow external sources to connect.

There is also a check box for Block All Incoming Connections. This feature allows you to connect to networks that are not secure. When Block All Incoming Connections is enabled, exceptions are ignored and no notification will be given when an application is blocked by Windows Firewall.

The Exceptions tab of the Windows Firewall Settings dialog box, shown in Figure 6.12, allows you to define which programs and services should be allowed to pass through the Windows Firewall. You can select from a defined list of programs and services or you can use the Add Program and Add Port buttons to customize your exceptions. Finally, you can select whether you want Windows Firewall to notify you when a program is blocked.

Some useful predefined exceptions include File and Printer Sharing, Microsoft Windows Fax and Scan, Performance Logs and Alerts, Remote Assistance, Remote Desktop, Windows Media Player, and Windows Meeting Space. If you notice that an application is not able to communicate over the network, you should check to ensure that the appropriate exception has been enabled.

FIGURE 6.12 Windows Firewall Settings dialog box, Exceptions tab



Take great care in enabling exceptions. Exceptions allow traffic to pass through the firewall, which could expose your computer to risk. Remember that the Block All Incoming Connections setting will ignore all exceptions.

The Advanced tab of the Windows Firewall Settings dialog box, shown in Figure 6.13, allows you to customize the firewall settings for specific connections (as opposed to the settings being globally set). You can also restore the Windows Firewall settings to a default state.

Windows Firewall with Advanced Security

You can configure more advanced settings by configuring Windows Firewall with Advanced Security (WFAS). To access Windows Firewall with Advanced Security, click Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools, then double-click Windows Firewall with Advanced Security. The Windows Firewall with Advanced Security dialog box will appear, as shown in Figure 6.14.

The scope pane to the left shows that you can set up specific inbound and outbound rules, connection security rules, and monitoring rules. The central area shows an overview of the firewall's status, as well as the current profile settings.

FIGURE 6.13 Windows Firewall Settings dialog box, Advanced tab

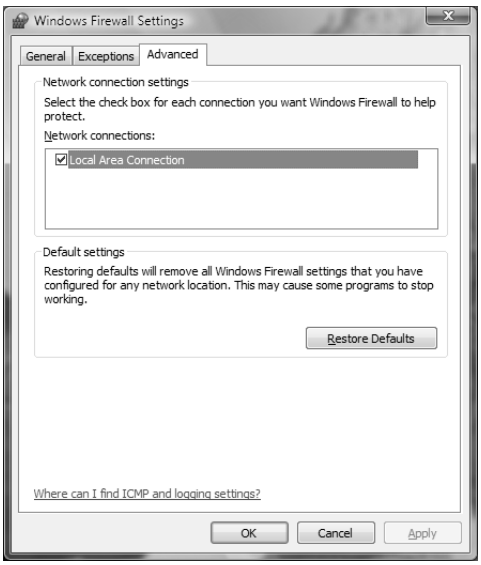
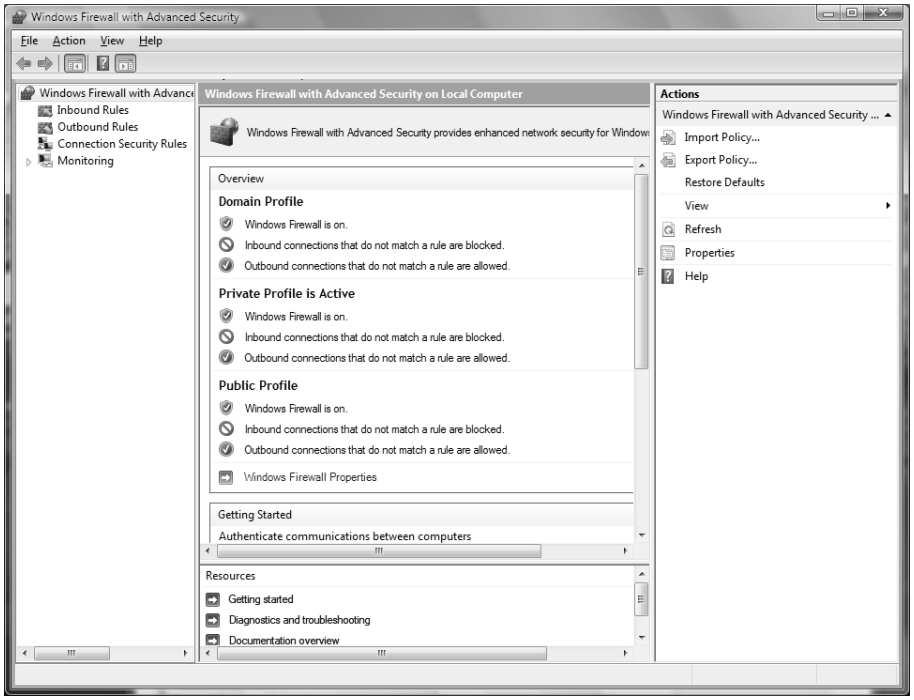


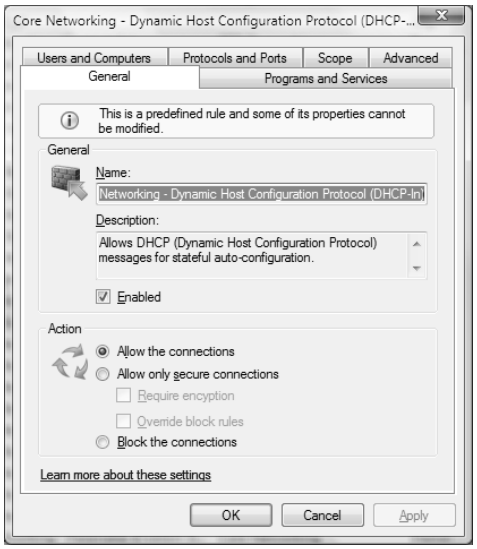
FIGURE 6.14 Windows Firewall with Advanced Security



Inbound and Outbound Rules

Inbound and outbound rules consist of many preconfigured rules that can be enabled or disabled. Obviously, inbound rules monitor inbound traffic, and outbound rules monitor outbound traffic. By default, most are disabled. Double-clicking on a rule will bring up its Properties dialog box, as shown in Figure 6.15.

FIGURE 6.15 An inbound rule's Properties dialog box



You can filter the rules to make them easier to view. Filtering can be performed based on the profile the rule affects, whether the rule is enabled or disabled, or based on the rule group.

If you can't find a rule that is appropriate for your needs, you can create a new rule by right-clicking Inbound Rules or Outbound Rules in the scope pane, then selecting New Rule. The New Inbound (or Outbound) Rule Wizard will launch, and you will be asked whether you want to create a rule based on a particular program, protocol or port, predefined category, or custom settings.

In Exercise 6.9, you will create a new inbound rule that will allow only encrypted TCP traffic. This exercise assumes you have completed all the previous exercises in this chapter.

EXERCISE 6.9

Inbound Rule Creation in Windows Firewall with Advanced Security

1. Select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools, then double-click Windows Firewall with Advanced Security.
2. Right-click Inbound Rules and select New Rule.

EXERCISE 6.9 *(continued)*

3. Choose a Rule Type. For this exercise, let's choose Custom so that we can see all the options available to us, then click Next.
4. Choose the programs or services that are affected by this rule. For this exercise, let's choose All Programs, then click Next.
5. Choose the protocol type, as well as the local and remote port numbers that are affected by this rule. For this exercise, let's choose TCP, and ensure that All Ports is selected for both Local Port and Remote Port. Click Next to continue.
6. Choose the local and remote IP addresses that are affected by this rule. Let's choose Any IP Address for both local and remote, then click Next.
7. Specify whether this rule will allow the connection, allow the connection only if it is secure, allow the connection only if it is encrypted, override blocking rules, or block the connection. Let's select the options Allow the Connection If It Is Secure, and Require the Connections to Be Encrypted, then click Next.
8. Specify whether connections should be allowed only from certain computers or certain users. You can experiment with these options if you want. Then, click Next to continue.
9. Choose which network profiles will be affected by this rule. Select one or more profiles and click Next to continue.
10. Give your profile a name and description, then click Finish. Your custom rule will appear in the list of Inbound Rules, and the rule will be enabled.
11. Double-click on your newly created rule. Notice that you can change the options that you previously configured.
12. Disable the rule by selecting the General tab, then clearing the Enabled check box.

Connection Security Rules

Connection Security Rules are used to configure how and when authentication occurs. These rules do not specifically allow connections; that's the job of inbound and outbound rules. You can configure the following connection security rules:

- Isolation: To restrict a connection based on authentication criteria
- Authentication Exemption: To specify computers that are exempt from authentication requirements
- Server-to-Server: To authenticate connections between computers
- Tunnel: To authenticate connections between gateway computers
- Custom

Monitoring

The Monitoring section of the scope pane shows detailed information about the firewall configurations for the Domain Profile, Private Profile, and Public Profile settings. These network location profiles determine what settings are enforced for private networks, public networks, and networks connected to a domain.

Network location profiles are covered in greater detail in Chapter 8, "Configuring Network Connectivity."

Using Windows Defender

These days, having a firewall and an antivirus program just isn't enough. Spyware is becoming more widespread, more sophisticated, and more dangerous. Users can unintentionally pick up spyware by visiting websites, or by installing an application in which spyware is bundled. Even worse, spyware cannot typically be uninstalled. Thus, an antispyware application is also required to ensure that your computer remains protected.

Windows Vista comes with an antispyware application called Windows Defender, formerly known as Microsoft AntiSpyware. Windows Defender offers real-time protection from spyware and other unwanted software. You can also configure Windows Defender to scan for spyware on a regular basis.

Like antivirus programs, Windows Defender relies on definitions, which are used to determine whether a file contains spyware. Out-of-date definitions can cause Windows Defender to not detect some spyware. Windows Update is used to regularly update the definitions used by Windows Defender so that the latest spyware can be detected. You can also configure Windows Defender to manually check for updates using Windows Update.

To access Windows Defender, click Start ➢ All Programs ➢ Windows Defender. You can also access Windows Defender through the Control Panel. Figure 6.16 shows Windows Defender. The status appears at the bottom of the screen, which includes time of the last scan, the scan schedule, the real-time protection status, and the definition version.

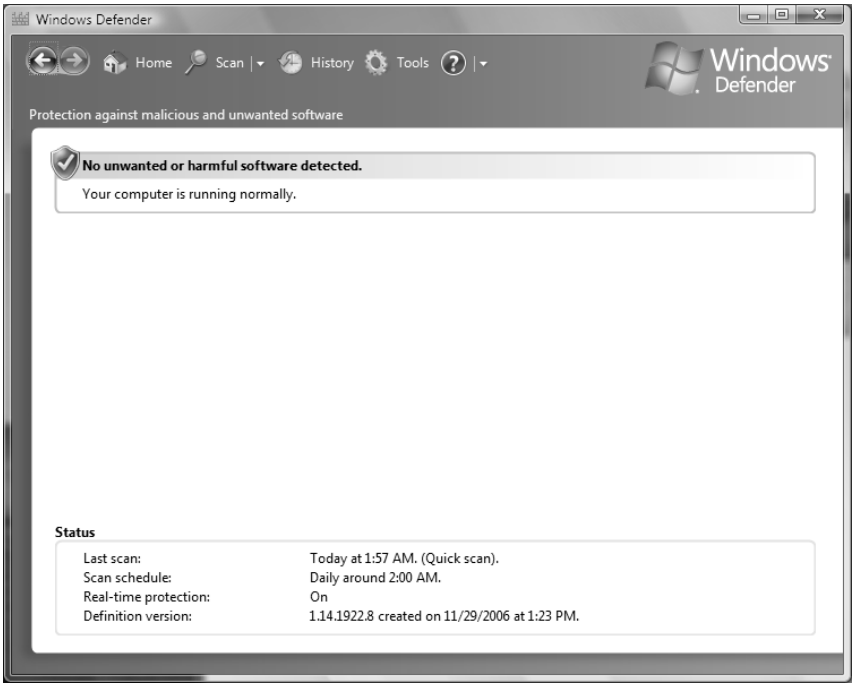
Performing a Manual Scan

You can configure Windows Defender to perform a manual scan of your computer at any time. There are three different types of scans that can be performed:

- Quick Scan checks only where spyware is most likely to be found.
- Full Scan checks all memory, running processes, and folders.
- Custom Scan checks only the drives and folders that you select.

By default, Windows Defender performs a Quick Scan every morning at 2 AM. You can change this setting by using the Tools menu option.

FIGURE 6.16 Windows Defender



Programs are classified into five spyware alert levels:

- Severe
- High
- Medium
- Low
- Not Yet Classified

Depending on the alert level, you can choose to have Windows Defender ignore, quarantine, remove, or always allow software.

Configuring Windows Defender

The Tools menu option is used to configure Windows Defender. As shown in Figure 6.17, the following items can be accessed through the Tools menu:

- Options
- Microsoft SpyNet
- Quarantined Items

FIGURE 6.17 Windows Defender Tools menu

- Allowed Items
- Software Explorer
- Windows Defender Website

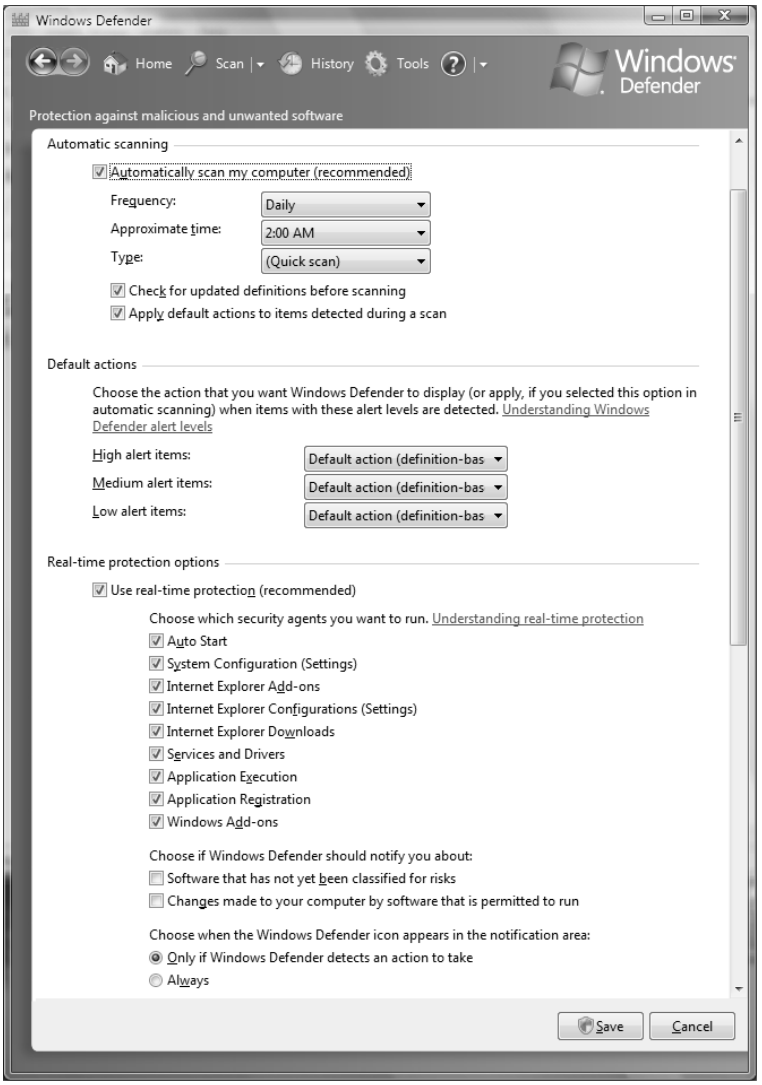
Options

Clicking Options on the Tools menu will enable you to configure the default behavior of Windows Defender, as shown in Figure 6.18. You can configure the following options:

- Automatic Scanning configures Windows Defender to automatically scan, how often automatic scans should occur, the time that scans will occur, and the type of scan to perform. You can also configure whether definitions should be updated before scanning, and whether the default actions should be taken on any spyware that is found.
- Default Actions configures the actions Windows Defender should take on High, Medium, and Low Alert items. You can configure each level so that Windows Defender can take the default action for that level, always remove the item, or always ignore the item.
- Real-Time Protection configures whether real-time protection is enabled, which security agents you want to run, how you should be notified about threats, and whether a Windows Defender icon is displayed in the notification area.

- Advanced Options configures whether archived files and folders are scanned, whether heuristics are used to detect unanalyzed software, whether a restore point is created before removing spyware, and file locations that are exempt from scanning.
- Administrator Options configures whether Windows Defender is enabled, and whether standard users can use Windows Defender to perform scans and change settings.

FIGURE 6.18 Windows Defender Options



Microsoft SpyNet

Microsoft SpyNet is an online community that can help you know how others respond to software that has not yet been classified by Microsoft. Participation in SpyNet is voluntary, and subscription to SpyNet is free. If you choose to volunteer, your choices will be added to the community so that others can learn from your experiences.

To join the SpyNet community, click Microsoft SpyNet on the Tools menu, then choose either a basic or advanced membership. The level of membership will specify how much information is sent to Microsoft when potentially unwanted software is found on your computer.

By default, a basic membership is selected, but you can choose to not participate in SpyNet by selecting the appropriate radio button. If you choose not to participate, no information will be sent to Microsoft, and Windows Defender will not alert you regarding unanalyzed software.

Even if you do not sign up for Microsoft SpyNet, you can still use heuristics scanning (select Tools ➢ Options) to detect potentially dangerous behavior in unanalyzed software.

Quarantined Items

Software that has been quarantined by Windows Defender is placed in Quarantined Items. Quarantined software will remain here until you remove it. If you find that a legitimate application is accidentally removed by Windows Defender, you can restore the application from Quarantined Items.

Allowed Items

Software that has been marked as allowed will be added to the Allowed Items list. Only trusted software should be added to this list. Windows Defender will not alert you regarding any software found on the Allowed Items list. If you find that a potentially dangerous application has been added to the Allowed Items list, you can remove it from the list so that Windows Defender can detect it.

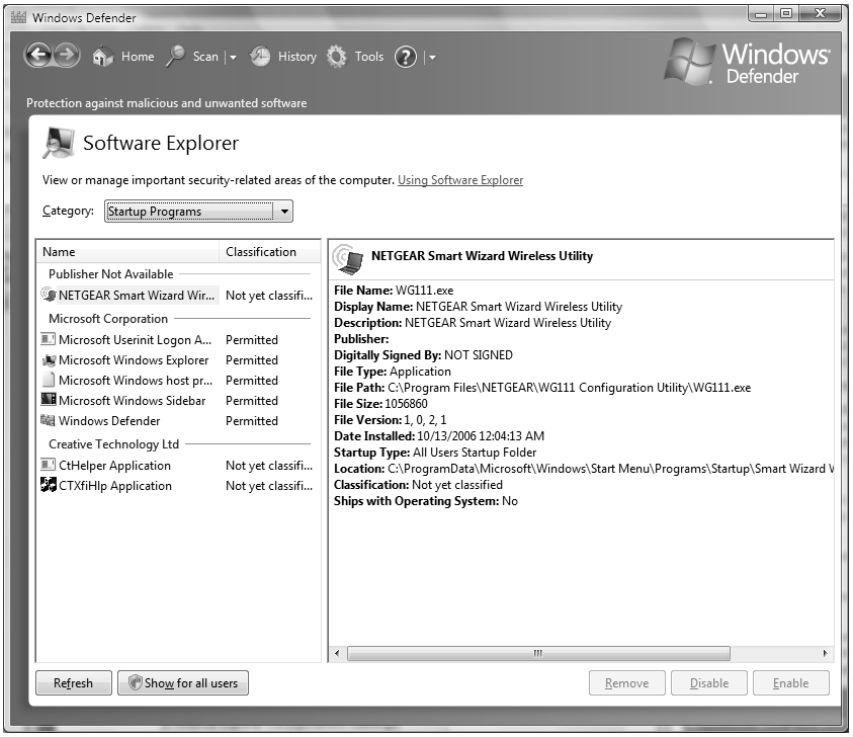
Software Explorer

Software Explorer, shown in Figure 6.19, shows a list of installed software as well as the software's classification level. You can choose to view Startup Programs, Currently Running Programs, Network Connected Programs, and Winsock Service Providers. Detailed data can be displayed for each application.

Windows Defender Website

Clicking Windows Defender Website will open up Internet Explorer and take you to the Windows Defender Website. Here, you can find information on Windows Defender, spyware, and security.

FIGURE 6.19 Software Explorer



History

The History menu option is used to see what actions have been taken by Windows Defender. Information is included about each application, the alert level, the action taken, the date, and the status. Information will be retained until you click the Clear History button.

Using BitLocker Drive Encryption

To prevent individuals from stealing your computer and viewing personal and sensitive data found on your hard disk, some editions of Windows Vista come with a new feature called BitLocker Drive Encryption. BitLocker encrypts the entire system drive. New files added to this drive are encrypted automatically, and files moved from this drive to another drive or computer are decrypted automatically.

Only Windows Vista Enterprise and Ultimate include BitLocker Drive Encryption.

Only the operating system drive (usually C:) can be encrypted with BitLocker. Files on other drives must be encrypted using another method, such as Encrypting File System (EFS).

BitLocker uses a Trusted Platform Module (TPM) version 1.2 or higher to store the security key. A TPM is a chip that is found in newer computers. If you do not have a computer with a TPM, you can store the key on a removable USB drive. The USB drive will be required each time you start the computer so that the system drive can be decrypted.

If the TPM discovers a potential security risk, such as a disk error, or changes made to BIOS, hardware, system files, or startup components, the system drive will not be unlocked until you enter the 48-digit BitLocker recovery password or use a USB drive with a recovery key.

The BitLocker recovery password is very important. Do not lose it, or you may not be able to unlock the drive. Even if you do not have a TPM, be sure to keep your recovery password in case your USB drive becomes lost or corrupted.

BitLocker requires that you have a hard disk with at least two partitions, both formatted with NTFS. One partition will be the system partition that will be encrypted. The other partition will be the active partition that is used to start the computer; this partition will remain unencrypted.

Managing File and Folder Security

Administrators must have basic file management skills, including the ability to create a well-defined, logically organized directory structure and maintain that structure. File and folder security defines what access a user has to local resources. You can limit access by applying security for files and folders. You should know what NTFS security permissions are and how they are applied.

A powerful feature of networking is the ability to allow network access to local folders. In Windows Vista, it is very easy to share folders. You can also apply security to shared folders in a manner that is similar to applying NTFS permissions. Once you share a folder, users with appropriate access rights can access the folders through a variety of methods.

Folder Options

The Windows Vista Folder Options dialog box allows you to configure many properties associated with files and folders, such as what you see when you access folders and how

Windows searches through files and folders. To open the Folder Options dialog box, click Start ➢ Computer, then select Folder and Search Options under the Organize drop-down list. You can also access Folder Options through its icon in Control Panel ➢ Classic View ➢ Folder Options. The Folder Options dialog box has three tabs: General, View, and Search. The options on each of these tabs are described in the following sections.

Folder General Options

The General tab of the Folder Options dialog box, shown in Figure 6.20, includes the following options:

- A choice of showing a preview of each file or using the Windows Classic View for displaying folders
- Whether folders are opened all in the same window when a user is browsing folders or each folder is opened in a separate window
- Whether a user opens items with a single mouse click or a double-click

Folder View Options

The options on the View tab of the Folder Options dialog box, shown in Figure 6.21, are used to configure what users see when they open files and folders. For example, you can change the default setting so that hidden files and folders are displayed. Table 6.7 describes the View tab options.

FIGURE 6.20 The General tab of the Folder Options dialog box

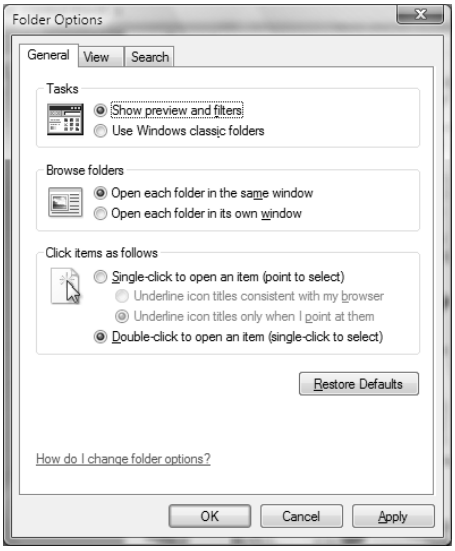


FIGURE 6.21 The View tab of the Folder Options dialog box

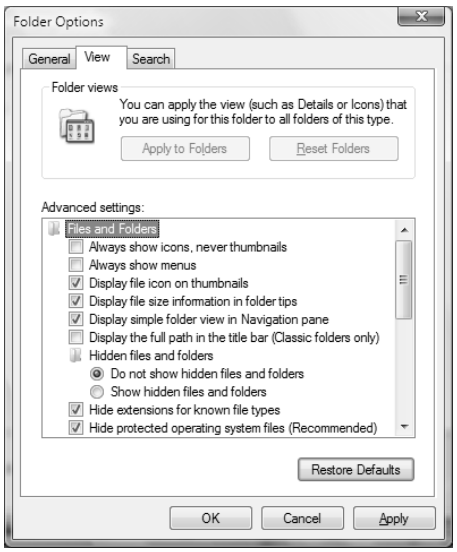


TABLE 6.7 Folder View Options

Option	Description	Default Value
Always Show Icons, Never Thumbnails	Shows icons for files instead of thumbnail previews.	Not selected
Always Show Menus	Shows the File, Edit, View, Tools, and Help menus when browsing for files.	Not selected
Display File Icon on Thumbnails	Displays the file icon on thumbnails.	Enabled
Display File Size Information in Folder Tips	Specifies whether the file size is automatically displayed when you hover your mouse over a folder.	Enabled
Display Simple Folder View in Navigation Pane	Specifies whether lines that connect folders and subfolders are shown in the Navigation Pane; Simple Folder View does not show these lines.	Enabled

TABLE 6.7 Folder View Options *(continued)*

Option	Description	Default Value
Display the Full Path in the Title Bar (Classic Folders Only)	Specifies whether the title bar shows an abbreviated path of your location. Enabling this option displays the full path, such as `C:\Word Documents\Sybex\Windows Vista Book\Chapter 6` as opposed to showing an abbreviated path such as `Chapter 6`.	Not selected
Hidden Files and Folders	Specifies whether files and folders with the Hidden attribute are listed. Choosing Show Hidden Files and Folders displays these items.	Do Not Show Hidden Files and Folders
Hide Extensions for Known File Types	By default, filename extensions, which identify known file types (such as `.doc` for Word files and `.xls` for Excel files) are not shown. Disabling this option displays all filename extensions.	Enabled
Hide Protected Operating System Files (Recommended)	By default, operating system files are not shown, which protects operating system files from being modified or deleted by a user. Disabling this option displays the operating system files.	Enabled
Launch Folder Windows in a Separate Process	By default, when you open a folder, it shares memory with the previous folders that were opened. Enabling this option opens folders in separate parts of memory, which increases the stability of Windows Vista but can slightly decrease the performance of the computer.	Not selected
Remember Each Folder's View Settings	By default, any folder display settings you make are retained each time the folder is reopened. Disabling this option resets the folder display settings to their defaults each time the folder is opened.	Enabled
Restore Previous Folder Windows at Logon	Specifies that if you leave folders open at logoff, they will be automatically reopened when you log on again.	Not selected
Show Drive Letters	Specifies whether drive letters are shown in the Computer folder. When disabled, only the name of the disk or device will be shown.	Enabled
Show Encrypted or Compressed NTFS Files in Color	Displays encrypted or compressed files in an alternate color when they are displayed in a folder window.	Enabled

TABLE 6.7 Folder View Options *(continued)*

Option	Description	Default Value
Show Pop-up Description for Folder and Desktop Items	Displays whether a pop-up tooltip is displayed when you hover your mouse over files and folders.	Enabled
Show Preview Handlers in Preview Pane	Shows the contents of files in the Preview pane.	Enabled
Use Check Boxes to Select Items	Adds a check box to each file and folder so that one or more of them may be selected. Actions can then be performed on selected items.	Not selected
Use Sharing Wizard (Recommended)	This option allows you to share a folder using a simplified sharing method.	Enabled
When Typing Into List View	Selects whether text is automatically typed into the Search Box or whether the typed item is selected in the view.	Select the Typed Item in the View

Search View Options

The options on the Search tab of the Folder Options dialog box, shown in Figure 6.22, are used to configure how Windows Vista searches for files. You can choose for Windows Vista to search by filename only, by filenames and contents, or a combination of the two, depending on whether indexing is enabled. You can also select from the following options:

- Include Subfolders
- Find Partial Matches
- Use Natural Language Searches
- Don't Use the Index When Searching the File System
- Include System Directories in Non-indexed Locations
- Include Compressed Files in Non-indexed Locations

To search for files and folders, click Start ➢ Search and type your query in the search box.

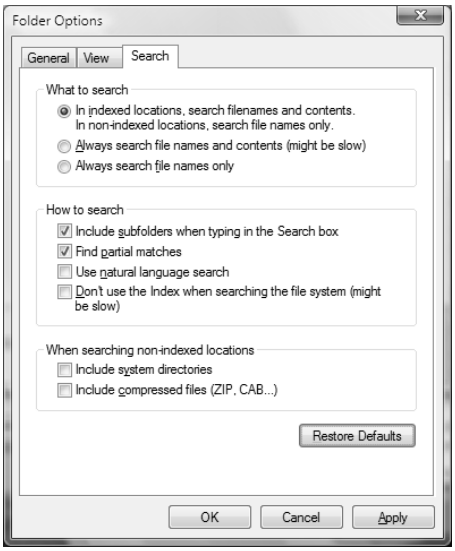
Securing Access to Files and Folders

On NTFS partitions, you can specify the access each user has to specific folders on the partition, based on the user's logon name and group associations. Access control consists of rights and permissions. A right (also referred to as a privilege) is an authorization to perform a specific action. Permissions are authorizations to perform specific operations on specific objects. The *owner* of an object or any user who has the necessary rights to modify permissions can apply permissions to NTFS objects. If permissions are not explicitly granted within NTFS,

then they are implicitly denied. Permissions can also be explicitly denied, which then overrides explicitly granted permissions.

The following sections describe design goals for access control, as well as how to apply NTFS permissions and some techniques for optimizing local access.

FIGURE 6.22 The Search tab of the Folder Options dialog box



Design Goals for Access Control

Before you start applying NTFS permissions to resources, you should develop design goals for access control as a part of your overall security strategy. Basic security strategy suggests that you provide each user and group with the minimum level of permissions needed for job functionality. Some of the considerations when planning access control include the following:

- Defining the resources that are included within your network—in this case, the files and folders residing on the file system
- Defining which resources will put your organization at risk; this includes defining the resources and defining the risk of damage if the resource was compromised
- Developing security strategies that address possible threats and minimize security risks
- Defining groups that security can be applied to based on users within the group membership who have common access requirements, and applying permissions to groups, as opposed to users
- Applying additional security settings through Group Policy, if your Windows Vista clients are part of an Active Directory network
- Using additional security features, such as EFS, to provide additional levels of security or file auditing to track access to critical files and folders

Applying NTFS Permissions

NTFS permissions control access to NTFS files and folders. This is based on the technology that was originally developed for Windows NT. Ultimately, the person who owns the object has complete control over the object. You configure access by allowing or denying NTFS permissions to users and groups. Normally, NTFS permissions are cumulative, based on group memberships if the user has been allowed access. However, if the user had been denied access through user or group membership, those permissions override the allowed permissions. Windows Vista offers six levels of NTFS permissions:

Full Control This permission allows the following rights:

- Traverse folders and execute files (programs) in the folders. The ability to traverse folders allows you to access files and folders in lower subdirectories, even if you do not have permissions to access specific portions of the directory path.
- List the contents of a folder and read the data in a folder's files.
- See a folder's or file's attributes.
- Change a folder's or file's attributes.
- Create new files and write data to the files.
- Create new folders and append data to the files.
- Delete subfolders and files.
- Delete files.
- Compress files.
- Change permissions for files and folders.
- Take ownership of files and folders.

If you select the Full Control permission, all permissions will be checked by default and can't be unchecked.

Modify This permission allows the following rights:

- Traverse folders and execute files in the folders.
- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.
- Change a file's or folder's attributes.
- Create new files and write data to the files.
- Create new folders and append data to the files.
- Delete files.

If you select the Modify permission, the Read & Execute, List Folder Contents, Read, and Write permissions will be checked by default and can't be unchecked.

Read & Execute This permission allows the following rights:

- Traverse folders and execute files in the folders.
- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.

If you select the Read & Execute permission, the List Folder Contents and Read permissions will be checked by default and can't be unchecked.

List Folder Contents This permission allows the following rights:

- Traverse folders.
- List the contents of a folder.
- See a file's or folder's attributes.

Read This permission allows the following rights:

- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.
- View ownership.

Write This permission allows the following rights:

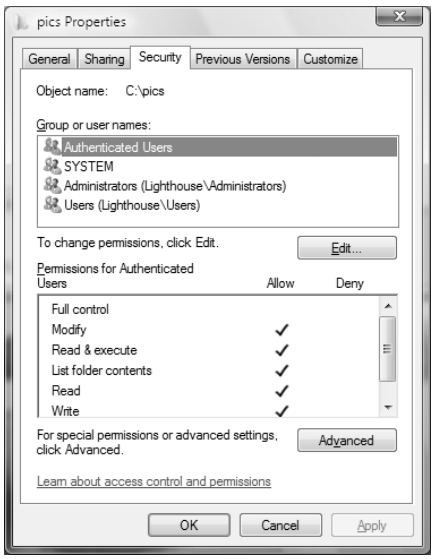
- Overwrite a file.
- View file ownership and permissions.
- Change a file's or folder's attributes.
- Create new files and write data to the files.
- Create new folders and append data to the files.

Any user with Full Control access can manage the security of a folder. However, to access folders, a user must have physical access to the computer as well as a valid logon name and password. By default, regular users can't access folders over the network unless the folders have been shared. Sharing folders is covered in the "Creating Shared Folders" section later in this chapter.

To apply NTFS permissions, right-click the file or folder to which you want to control access, select Properties from the context menu, then select the Security tab. The Security tab lists the users and groups that have been assigned permissions to the file or folder. When you click a user or group in the top half of the dialog box, you see the permissions that have been allowed or denied for that user or group in the bottom half, as shown in Figure 6.23.

The process for configuring NTFS permissions for files and folders is the same. The examples in this chapter use a folder, since NTFS permissions are most commonly applied at the folder level.

FIGURE 6.23 The Security tab of the folder Properties dialog box



In the following subsections you will learn how to implement NTFS permissions and how to control permission inheritance.

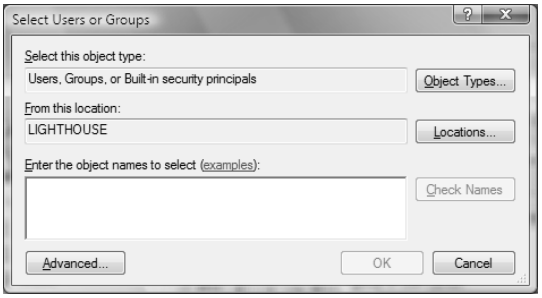
Adding and Removing User and Group NTFS Permissions

To manage NTFS permissions, take the following steps:

1. Right-click the file or folder to which you want to control access, select Properties from the context menu, and click the Security tab.
2. Click the Edit button to modify permissions.
3. Click the Add button to open the Select Users or Groups dialog box, as shown in Figure 6.24. You can select users from the computer's local database or from the domain you are in (or trusted domains) by typing in the user or group name in the Enter the Object Names to Select portion of the dialog box and clicking OK.
4. You return to the Security tab of the folder Properties dialog box. Highlight a user or group in the top list box, and in the Permissions list, specify the NTFS permissions to be allowed or denied. When you have finished, click OK.

Through the Advanced button of the Security tab, you can configure more granular NTFS permissions, such as Traverse Folder and Read Attributes permissions.

FIGURE 6.24 The Select Users or Groups dialog box



To remove the NTFS permissions for a user, computer, or group, highlight that entity in the Security tab and click the Remove button.

Be careful when you remove NTFS permissions. You won't be asked to confirm their removal, as you are when deleting most other types of items in Windows Vista.

Controlling Permission Inheritance

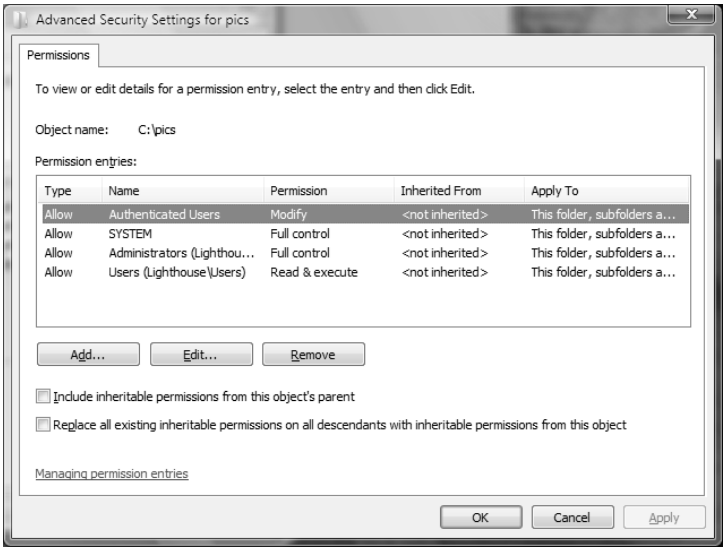
Normally, the directory structure is organized in a hierarchical manner. This means you are likely to have subfolders in the folders to which you apply permissions. In Windows Vista, by default, the parent folder's permissions are applied to any files or subfolders in that folder, as well as any subsequently created objects. These are called *inherited permissions*.

In Windows NT 4, by default, files in a folder do inherit permissions from the parent folder, but subfolders do not inherit parent permissions. In Windows 2000, XP Professional, and Windows Vista, the default is for the permissions to be inherited by subfolders.

You can specify how permissions are inherited by subfolders and files through the Advanced options from the Security tab of a folder's Properties dialog box by clicking the Advanced button. This calls up the Permissions tab of the Advanced Security Settings dialog box. To edit these options, click Edit. The options that can be selected in Figure 6.25 include the following:

- Include Inheritable Permissions from This Object's Parent
- Replace All Existing Inheritable Permissions on All Descendants with Inheritable Permissions from This Object

FIGURE 6.25 The Permissions tab of the Advanced Security Settings dialog box



If an Allow or a Deny check box in the Permissions list on the Security tab has a shaded check mark, this indicates that the permission was inherited from an upper-level folder. If the check mark is not shaded, it means the permission was applied at the selected folder. This is known as an *explicitly assigned permission*. Knowing which permissions are inherited and which are explicitly assigned is useful when you need to troubleshoot permissions.

Understanding Ownership and Security Descriptors

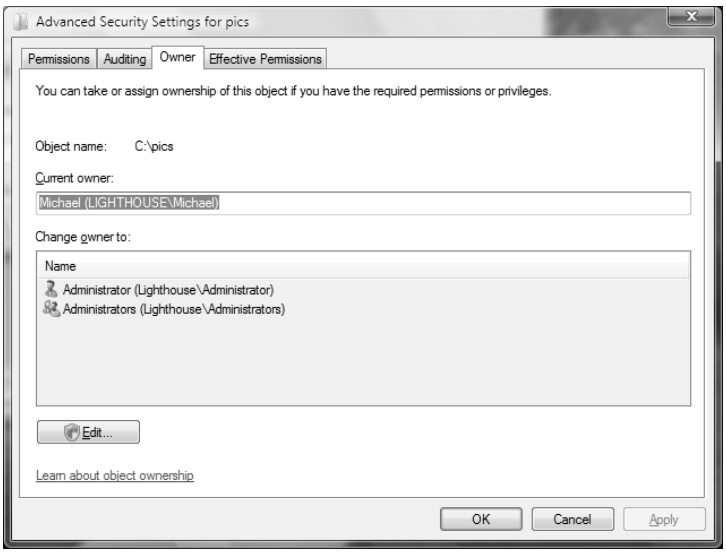
When an object is initially created on an NTFS partition, an associated security descriptor is created. A security descriptor contains the following information:

- The user or group that owns the object
- The users and groups that are allowed or denied access to the object
- The users and groups whose access to the object will be audited

After an object is created, the owner of the object has full permissions to change the information in the security descriptor, even for members of the Administrators group. You can view the owner of an object from the Security tab of the specified folder's Properties (as shown in Figure 6.23) and clicking the Advanced button. Then click the Owner tab to see who the owner of the object is, as shown in Figure 6.26. From this dialog box you can change the owner of the object.

Although the owner of an object can set the permissions of an object so that the Administrator can't access the object, the Administrator or any member of the Administrators group can take ownership of an object and thus manage the object's permissions. When you take ownership of an object, you can specify whether you want to replace the owner on subdirectories and objects of the object.

FIGURE 6.26 The Owner tab of the Advanced Security Settings dialog box



Real World Scenario

Using the Take Ownership Option

You are the administrator of a large network. The manager of the accounting department, Will, set up a series of files and folders with a high level of security. Will was the owner of these and all of the associated files and folders. When he set up NTFS security for his files and folders, he removed access for everyone, including the Administrators group. Will recently left the company, and Kevin has been hired to take over the accounting manager's job. When Kevin tries to access Will's files, he can't. When you log on as Administrator, you also can't access any of the files.

In this case, you should access the Owner tab of the parent folder for the files and folders and change the owner to Kevin. You should ensure that you check Replace Owner on Subcontainers and Objects, and Kevin will now be able to have Full Control permissions to the resources.

From a command prompt, you can see who the owner of a directory is by typing **`dir /q`**.

Determining Effective Permissions

To determine a user's *effective rights* (the rights the user actually has to a file or folder), add all of the permissions that have been allowed through the user's assignments based on that user's username and group associations. After you determine what the user is allowed, you subtract any permissions that have been denied the user through the username or group associations.

As an example, suppose that user Marilyn is a member of both the Accounting and Execs groups. The following assignments have been made to the Accounting group permissions:

Permission	Allow	Deny
Full Control		
Modify	X	
Read & Execute	X	
List Folder Contents		
Read		
Write		

The following assignments have been made to the Execs group permissions:

Permission	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read	X	
Write		

To determine Marilyn's effective rights, you combine the permissions that have been assigned. The result is that Marilyn's effective rights are Modify, Read & Execute, and Read.

As another example, suppose that user Dan is a member of both the Sales and Temps groups. The following assignments have been made to the Sales group permissions:

Permission	Allow	Deny
Full Control		
Modify	X	
Read & Execute	X	

Permission	Allow	Deny
List Folder Contents	X	
Read	X	
Write	X	

The following assignments have been made to the Temps group permissions:

Permission	Allow	Deny
Full Control		
Modify		X
Read & Execute		
List Folder Contents		
Read		
Write		X

To determine Dan's effective rights, you start by seeing what Dan has been allowed: Modify, Read & Execute, List Folder Contents, Read, and Write permissions. You then remove anything that he is denied: Modify and Write permissions. In this case, Dan's effective rights are Read & Execute, List Folder Contents, and Read.

Viewing Effective Permissions

If permissions have been applied at the user and group levels, and inheritance is involved, it can sometimes be confusing to determine what the effective permissions are. To help identify which effective permissions will actually be applied, you can view them from the Effective Permissions tab of Advanced Security Settings, or you can use the ICACLS command-line utility.

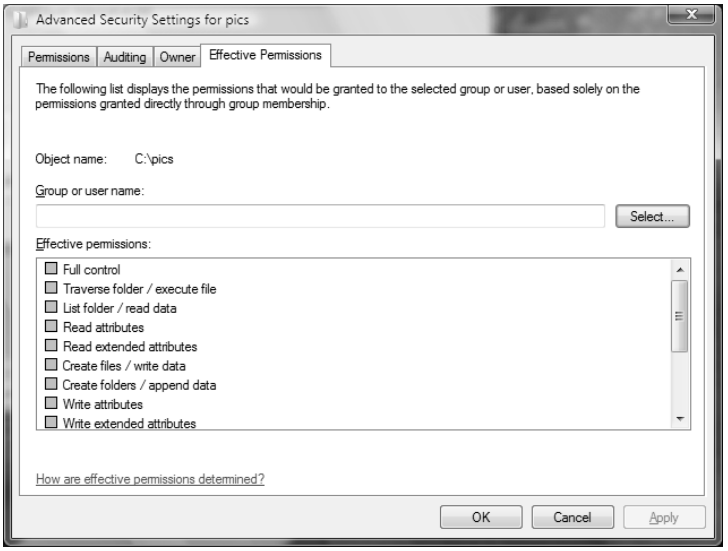
Figure 6.27 shows the Effective Permissions tab of Advanced Security Settings.

To see what the effective permissions are for a user or group, you click the Select button and then type in the user or group name. Then click OK. If a box is checked and not shaded, then explicit permissions have been applied at that level. If the box is shaded, then the permissions to that object were inherited.

The ICACLS command-line utility can also be used to display or modify user access rights. The options associated with the `ICACLS` command are as follows:

- `/grant` grants permissions.
- `/remove` revokes permissions.
- `/deny` denies permissions.
- `/setintegritylevel` sets an integrity level of Low, Medium, or High.

FIGURE 6.27 The Effective Permissions tab of the Advanced Security Settings dialog box



The ICACLS command has replaced the CACLS command.

Determining NTFS Permissions for Copied or Moved Files

When you copy or move NTFS files, the permissions that have been set for those files might change. The following guidelines can be used to predict what will happen:

- If you move a file from one folder to another folder on the same volume, the file will retain the original NTFS permissions.
- If you move a file from one folder to another folder between different NTFS volumes, the file is treated as a copy and will have the same permissions as the destination folder.
- If you copy a file from one folder to another folder on the same volume or on a different volume, the file will have the same permissions as the destination folder.
- If you copy or move a file or folder to a FAT partition, it will not retain any NTFS permissions.

FAT partitions cannot be secured using NTFS permissions.

Managing Network Access

Sharing is the process of allowing network users to access a folder located on a Windows Vista computer. A network share provides a single location to manage shared data used by many users. Sharing also allows an administrator to install an application once, as opposed to installing it locally at each computer, and to manage the application from a single location.

The following sections describe how to create and manage *shared folders*, configure *share permissions*, and provide access to shared resources.

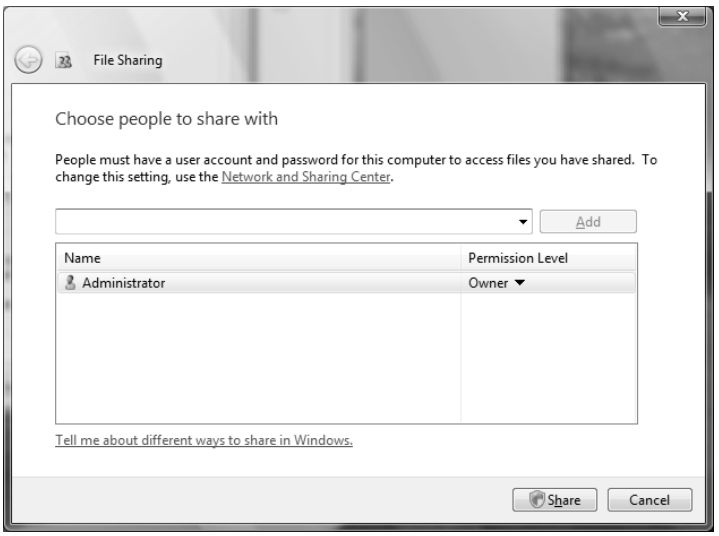
Creating Shared Folders

You can share a folder in two ways. To use the Sharing Wizard, right-click a folder and select Share. If the Sharing Wizard feature is enabled, you will see the File Sharing screen, as shown in Figure 6.28. Here, you can add local users and specify one of the following permission levels:

- Owner
- Co-Owner
- Contributor
- Reader

However, you cannot use the Sharing Wizard to share resources with domain users. To share a folder with domain users, you should right-click the folder and select Properties, then select the Sharing tab, as shown in Figure 6.29.

FIGURE 6.28 The Sharing Wizard



The Share button will take you to the Sharing Wizard. To configure Advanced Sharing, click the Advanced Sharing button, which will open up the Advanced Sharing dialog box, as shown in Figure 6.30.

When you share a folder, you can configure the options listed in Table 6.8.

FIGURE 6.29 The Sharing tab of a folder's Properties dialog box

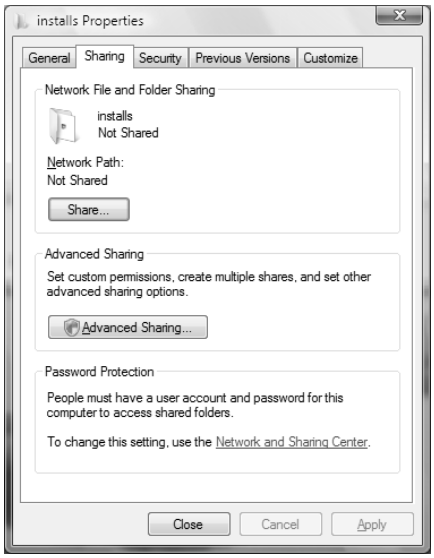


FIGURE 6.30 The Advanced Sharing dialog box

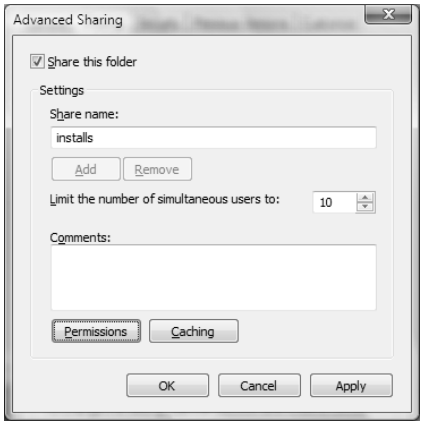


TABLE 6.8 Share Folder Options

Option	Description
Share This Folder	Makes the folder available through local access and network access
Share Name	A descriptive name by which users will access the folder
Comments	Additional descriptive information about the share (optional)
Limit the Number of Simultaneous Users To	The maximum number of connections to the share at any one time (no more than 10 users can simultaneously access a share on a Windows Vista computer)
Permissions	How users will access the folder over the network
Caching	How folders are cached when the folder is offline

If you share a folder and then decide that you do not want to share it, just deselect the Share This Folder check box.

You can easily tell that a folder has been shared by the group icon located at the bottom left of the folder icon.

The following also hold true:

- Only folders, not files, can be shared.
- Share permissions can be applied only to folders and not to files.
- If a folder is shared over the network and a user is accessing it locally, then share permissions will not apply to the local user; only NTFS permissions will apply.
- If a shared folder is copied, the original folder will still be shared but not the copy.
- If a shared folder is moved, the folder will no longer be shared.
- If the shared folder will be accessed by a mixed environment of clients including some that do not support long filenames, you should use the 8.3 naming format for files.
- Folders can be shared through the Net Share command-line utility.

Configuring Share Permissions

You can control users' access to shared folders by assigning share permissions. Share permissions are less complex than NTFS permissions and can be applied only to folders (unlike NTFS permissions, which can be applied to files and folders).

To assign share permissions, click the Permissions button in the Advanced Sharing dialog box. This brings up the Permissions dialog box, as shown in Figure 6.31.

You can assign three types of share permissions:

Full Control Allows full access to the shared folder.

Change Allows users to change data within a file or to delete files.

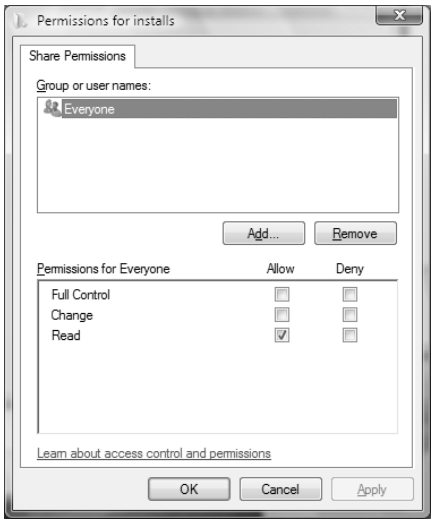
Read Allows a user to view and execute files in the shared folder.

Full Control is the default permission on shared folders for the Everyone group.

Shared folders do not use the same concept of inheritance as NTFS folders. If you share a folder, there is no way to block access to lower-level resources through share permissions.

When applying conflicting Share and NTFS permissions, the most restrictive permissions apply. Remember that Share and NTFS permissions are both applied only when a user is accessing a shared resource over a network. Only NTFS permissions apply to a user accessing a resource locally.

FIGURE 6.31 The Permissions dialog box



Summary

In this chapter, you learned how to define security for Windows Vista. We covered the following topics:

- The difference between LGPOs, which are applied at the local level, and GPOs, which are applied through a Windows 2000 or Windows 2003 domain, and how they are applied.
- Account policies, which control the logon process. The two types of account policies are password and account lockout policies.
- Local policies, which control what a user can do at the computer. The three types of local policies are audit, user rights, and security options policies.
- How to use the Group Policy Result Tool to analyze current configuration settings.
- How to use User Account Control.
- How to use Windows Security Center.
- How to use Windows Firewall and WFAS.
- How to use Windows Defender.
- How to use BitLocker Drive Encryption.
- How to configure NTFS permissions.
- How to configure Share permissions.

Exam Essentials

Understand how group policies are applied locally and through Active Directory. Know how group policies can be applied either locally through LGPOs or through Active Directory with GPOs. Understand how group policy is applied through the order of inheritance. Be able to use the Group Policy Result Tool to view how group policy is currently configured for a specific computer.

Know how to set local group policies. Understand the purpose of account policies and local policies. Know the purpose and implementation of account policies for managing password policies and account lockout policies. Understand the purpose and implementation of local policies and how they can be applied to users and groups for audit policies, user rights assignments, and security options.

Be familiar with User Account Control. Understand the purpose and features of User Account Control. Be familiar with Registry and file virtualization. Understand privilege escalation. Know the basics of the new UAC group policy settings.

Know how to use Windows Security Center. Be able to use Windows Security Center to monitor and configure settings for Windows Firewall, Automatic Updating, Malware Protection, and Other Security Settings.

Know how to use Windows Firewall. Be able to configure and use Windows Firewall and WFAS. Understand how exceptions work and how to block incoming connections.

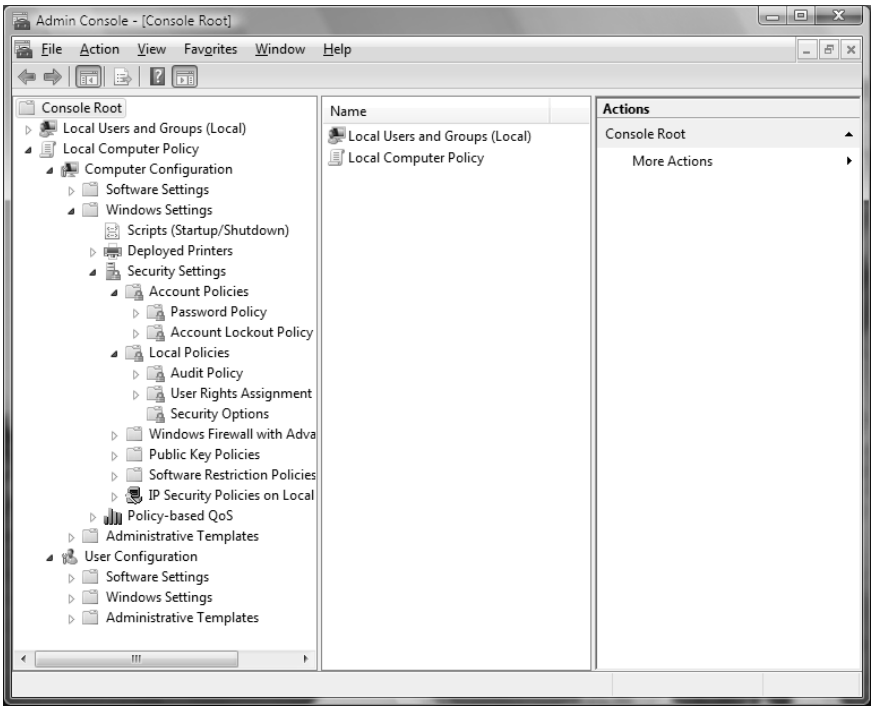
Know how to use Windows Defender. Be able to configure and use Windows Defender. Understand how Quarantine works. Know the purpose of Microsoft SpyNet.

Know how to use BitLocker Drive Encryption. Understand the purpose and requirements of BitLocker Drive Encryption. Know which editions of Windows Vista include BitLocker.

Understand NTFS and Share permissions. Be able to configure security permissions and know the difference between NTFS and Share permissions.

Review Questions

1. Your network's security has been breached. You are trying to redefine security so that a user cannot repeatedly attempt user logon with different passwords. To accomplish this, which of the following items (in the Local Security Settings dialog box shown here) should you define?



A. Password Policy

B. Account Lockout Policy

C. Audit Policy

D. Security Options

2. You are the network administrator for a Fortune 500 company. The accounting department has recently purchased a custom application for running financial models. To run properly, the application requires that you make some changes to the computer policy. You decide to deploy the changes through a Group Policy setting. You create an OU called Sales and apply the policy settings. When you log on as a member of the Sales OU and run the application, it is still not running properly. You suspect that the policy is not being applied properly because of a conflict somewhere with another Group Policy setting. What command should you run to see a listing of how the group policies have been applied to the computer and the user?

   A. GPResult

   B. GPOResult

   C. GPAudit

   D. GPInfo

3. You have a Windows Vista computer that is located in an unsecured area. You want to track usage of the computer by recording user logon and logoff events. To do this, which of the following auditing policies must be enabled?

   A. Audit Account Logon Events

   B. Audit Account Management

   C. Audit Process Tracking

   D. Audit System Events

4. You are the administrator for a printing company. After you configure the Password Must Meet Complexity Requirements policy, several users have problems when changing their passwords. Which of the following passwords meet the minimum complexity requirements?

   A. aBc-1

   B. Abcde!

   C. 1247445Np

   D. !@#$%^&*(-[]

5. You purchase Windows Vista Home Basic for your home computer because of the new features found in Windows Vista. After installation, you begin to implement Windows Vista's new features, but cannot find BitLocker Drive Encryption. On which editions of Windows Vista can you find this feature?

   A. Windows Vista Home Premium

   B. Windows Vista Professional

   C. Windows Vista Enterprise

   D. Windows Vista Ultimate

6. You are the system administrator for the ACME Corp. You have a computer that is shared by many users. You want to ensure that when users press Ctrl+Alt+Del to log on, they do not see the name of the last user. What do you configure?

   A. Set the security option Clear User Settings When Users Log Off.

   B. Set the security option Do Not Display Last User Name in Logon Screen.

   C. Set the security option Prevent Users from Seeing Last User Name.

   D. Configure nothing; this is the default setting.

7. You purchase a new Windows Vista computer. When configuring your Windows Firewall settings, you select the Block All Incoming Connections check box. You also configure an exception for Remote Desktop so that you can access the computer remotely. Which of the following actions will you not be able to perform?

   A. Connecting to the computer remotely using Remote Desktop

   B. Accessing Web pages

   C. Receiving e-mail

   D. Receiving instant messages

8. You have recently hired Al as an assistant for network administration. You have not decided how much responsibility you want Al to have. In the meantime, you want Al to be able to restore files on Windows Vista computers in your network, but you do not want Al to be able to run the backups. What is the minimum assignment that will allow Al to complete this task?

   A. Add Al to the Administrators group.

   B. Grant Al the Read right to the root of each volume he will back up.

   C. Add Al to the Backup Operators group.

   D. Grant Al the user right Restore Files and Directories.

9. You are the network administrator of a medium-sized company. Your company requires a fair degree of security and you have been tasked with defining and implementing a security policy. You have configured password policies so that users must change their passwords every 30 days. Which password policy would you implement if you want to prevent users from reusing passwords they have used recently?

   A. Passwords Must Be Advanced

   B. Enforce Password History

   C. Passwords Must Be Unique

   D. Passwords Must Meet Complexity Requirements

10. You have a network folder that resides on an NTFS partition on a Windows Vista computer. NTFS permissions and share permissions have been applied. Which of the following statements best describes how share permissions and NTFS permissions work together if they have been applied to the same folder?

A. The NTFS permissions will always take precedence.

B. The share permissions will always take precedence.

C. The system will look at the cumulative share permissions and the cumulative NTFS permissions. Whichever set is less restrictive will be applied.

D. The system will look at the cumulative share permissions and the cumulative NTFS permissions. Whichever set is more restrictive will be applied.

11. Your Active Directory structure consists of a domain called BRAINBEACON, which is part of a site called NASHVILLE. Your user's accounts are located within the BBUSERS OU. Each Windows Vista computer has a local policy set. You also configure site, OU, and domain GPOs. All of the GPOs are configured with the Block Inheritance option. What will occur when the resultant policy is applied?

A. GPO settings will be combined, but the OU GPO settings will be used in the event of conflict.

B. GPO settings will be combined, but the LGPO settings will be used in the event of conflict.

C. Only the OU GPO settings will be used.

D. Only the domain GPO settings will be used.

12. You configure your Windows Vista computer to run a nightly scan on your computer using Windows Defender. The next day, you find that one of your trusted applications has been removed by Windows Defender. Where can you go to restore your application?

A. Allowed Items

B. Quarantined Items

C. Software Explorer

D. SpyNet

13. Stacy is the network administrator for a library. Multiple users use the Windows Vista computer at the checkout desk, and Stacy wants to implement a variety of group policies to restrict their activities. In which order will local group policies be applied?

A. Local Computer Policy, Administrators/Non-Administrators Local Group Policy, User-Specific Group Policy

B. Administrators/Non-Administrators Local Group Policy, User-Specific Group Policy, Local Computer Policy

C. User-Specific Group Policy, Local Computer Policy, Administrators/Non-Administrators Local Group Policy

D. Administrators/Non-Administrators Local Group Policy, Local Computer Policy, User-Specific Group Policy

14. You are the network administrator for a large corporation. A new financial application is developed for the company. You install the application on Vince's Windows Vista computer. The application requires administrator privileges to run correctly. What should you do to enable Vince to use the financial application on a daily basis?

    A. Make Vince a member of the local Administrators group.

    B. Right-click the application's desktop shortcut and select Run as Administrator.

    C. Right-click the application's executable file and select Run as Administrator.

    D. Right-click the application's desktop shortcut, select Properties, select the Compatibility tab, and check the Run This Program as an Administrator check box.

15. You are the senior network administrator for a printing company. While training your junior network administrator, Trey, you notice that the User Account Control box is not appearing when he launches the Microsoft Management Console on a Windows Vista computer. You and Trey are both local administrators on the computer. What could cause this behavior to occur?

    A. Trey is logged in as himself.

    B. Trey is logged in as Administrator.

    C. Trey is logged in as you.

    D. The User Account Control: Admin Approval Mode for the Built-in Administrator Account policy is set to Enabled.

16. You are the network administrator for a bookstore. You install Windows Vista on a new computer. Before you connect the computer to the Internet, you want to ensure that the appropriate features are enabled. You open Windows Security Center and notice that there are features that require addressing. Which of the following features are not included with Windows Vista?

    A. Firewall protection

    B. Spyware protection

    C. Virus protection

    D. Automatic update protection

17. Sam is the network administrator for a small company. A user calls Sam and requires assistance installing some software on his new Windows Vista computer. Sam logs the user off and attempts to log on as the built-in Administrator account. However, the Administrator account is not available. What is the most likely reason why Sam cannot log onto the Administrator account?

    A. The built-in Administrator account was deleted by another administrator.

    B. The built-in Administrator account has been compromised.

    C. The built-in Administrator account does not exist in Windows Vista.

    D. The built-in Administrator account is disabled by default in Windows Vista.

18. A salesperson in your company purchases a new laptop with Windows Vista installed. She asks you to configure it for her. You create her a standard local user account. Which of the following tasks can she perform by default?

A. Changing date and time settings

B. Changing time zone settings

C. Checking Device Manager

D. Enabling parental controls

19. Ed is a newly hired network administrator. While configuring Group Policy, he configures settings for Internet Explorer under Local Computer Configuration, Local User Configuration, Domain Computer Configuration and Domain User Configuration. Which settings will take precedence?

A. Local Computer Configuration

B. Local User Configuration

C. Domain Computer Configuration

D. Domain User Configuration

20. You are the Active Directory administrator for your company. A Windows Vista computer has been purchased for the Finance department, and you want to monitor it for unauthorized access. You configure the Audit Object Access policy to audit both Success and Failure events. However, when you look at the Security Event Log a few days later, you do not see any entries related to file access. What is the most likely reason for this behavior?

A. Auditing has not been enabled for the appropriate files and folders.

B. A conflicting group policy setting is overriding your configuration.

C. Another administrator has disabled your group policy setting.

D. Object Access events are found in the System Event Log.

Answers to Review Questions

1. B. Account Lockout Policy, a subset of Account Policy, is used to specify options that prevent a user from attempting multiple failed logon attempts. If the Account Lockout Threshold value is exceeded, the account will be locked. The account can be reset based on a specified amount of time or through Administrator intervention.

2. A. The System Group Policy Result Tool is accessed through the GPResult command-line utility. The `gpresult` command displays the resulting set of policies that were enforced on the computer and the specified user during the logon process.

3. A. Audit Account Logon Events is used to track when a user logs on, logs off, or makes a network connection. You can configure auditing for success or failure, and audited events can be tracked through Event Viewer.

4. B, C. The password Abcde! meets complexity requirements because it is at least six characters long and contains uppercase letters, lowercase letters, and symbols. The password 1247445Np meets complexity requirements because it is at least six characters long and contains uppercase letters, lowercase letters, and numbers. Complex passwords must be at least six characters long and contain three of the four types of characters.

5. C, D. BitLocker Drive Encryption is found only in Windows Vista Enterprise and Windows Vista Ultimate. Windows Vista Enterprise is available only through Microsoft Software Assurance.

6. B. The security option Do Not Display Last User Name is used to prevent the last username in the logon screen from being displayed in the logon dialog box. This option is commonly used in environments where computers are used publicly.

7. A. You will not be able to connect to the computer remotely using Remote Desktop. The Block All Incoming Connections feature will ignore all exceptions. However, you will still be able to access most web pages, send and receive e-mail, and send and receive instant messages.

8. D. The Restore Files and Directories user right allows a user to restore files and directories, regardless of file and directory permissions. Assigning this user right is an alternative to making a user a member of the Backup Operators group.

9. B. The Enforce Password History policy allows the system to keep track of a user's password history for up to 24 passwords. This prevents a user from using the same password over and over again.

10. D. When both NTFS and share permissions have been applied, the system looks at the effective rights for NTFS and share permissions and then applies the most restrictive of the cumulative permissions. If a resource has been shared, and you access it from the local computer where the resource resides, then you will be governed only by the NTFS permissions.

11. C. The Block Inheritance option is used to specify that GPO settings will not be inherited from higher-level GPOs. Thus, because the OU policy is applied last, it will not inherit policy settings from the site, domain, and local GPOs.

12. B. You can restore your application from Quarantined Items. Applications that have been quarantined by Windows Defender will remain in Quarantined Items until you manually remove them.

13. A. The Local Computer Policy is applied first, the Administrators or Non-Administrators Local Group Policy is applied next, and the User-Specific Group Policy for that user is applied last. If there are any conflicts, then the last policy to be applied will take precedence. Thus, the User-Specific Group Policy would override any conflicting LGPO settings.

14. D. To enable Vince to use the financial application on a daily basis, you should right-click either the application's desktop shortcut or the application's executable file, select Properties, select the Compatibility tab, and check the Run This Program as an Administrator check box.

15. B. The UAC box will not appear when launching the MMC if you are logged in as the built-in Administrator account unless the User Account Control: Admin Approval Mode for the Built-in Administrator Account policy is set to Disabled. The UAC box will appear when launching the MMC as an administrator or as a standard user unless the appropriate User Account Control security option is configured to Elevate Without Prompting.

16. C. Virus protection is not included with Windows Vista and should be purchased separately. Windows Firewall, Windows Defender, and Windows Update are included with Windows Vista.

17. D. The most likely reason why Sam cannot log onto the Administrator account is because the built-in Administrator account is disabled by default in Windows Vista. However, it can be enabled through Local Users and Groups or by modifying the Accounts: Administrator Account Status GPO setting.

18. B. As a standard user, the salesperson can change time zone settings. Changing the date and time settings, checking Device Manager, and enabling parental controls require administrative privileges. Any action that requires administrative privileges will be marked with a shield icon.

19. C. The Domain Computer Configuration GPO settings will take precedence. Active Directory policies take precedence over local policies, and Computer Configuration policies take precedence over equivalent User Configuration policies.

20. A. The most likely reason why there are no file access entries in the Security Event Log is because you did not enable auditing for the appropriate files and folders. This behavior is true of print auditing as well.

Chapter

7

Configuring Disks

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring and Troubleshooting Post-Installation Configuration Issues**
  - Troubleshoot post-installation configuration issues.
- ✓ **Maintaining and Optimizing Systems That Run Windows Vista**
  - Troubleshoot reliability issues by using built-in diagnostic tools.
  - Configure Data Protection.

When you install Windows Vista, you designate the initial configuration for your disks. Through Windows Vista's utilities and features, you can change that configuration and perform disk-management tasks.

For file system configuration, it is recommended that you use NTFS, although you could also format the disk drive with FAT or FAT32. You can also update a FAT or FAT32 partition to NTFS. This chapter covers the features of each file system and how to use the Convert utility to upgrade to NTFS.

Another factor in disk management is choosing the configuration for your physical drives. Windows Vista supports basic and dynamic disks. When you install Windows Vista or upgrade from Windows XP using basic disks, the drives are configured as basic disks. Dynamic disks are supported by Windows Vista, Windows XP Professional, Windows 2000 (all versions), and Windows Server 2003 and allow you to create simple volumes, spanned volumes, and striped volumes.

Once you decide how your disks should be configured, you implement the disk configurations through the Disk Management utility. This utility helps you view and manage your physical disks and volumes. In this chapter, you will learn how to manage both types of storage and how to upgrade from basic storage to dynamic storage.

The other disk-management features covered in this chapter are data compression, data encryption, disk defragmentation, disk cleanup, and disk error checking.

The procedures for many disk-management tasks are the same for Windows Vista as they were for Windows XP Professional, Windows 2000 (all versions), and Windows Server 2003. The main difference is that Windows 2000 Server and Windows Server 2003 also support mirrored and RAID-5 volumes.

Configuring File Systems

Each partition (each *logical drive* that is created on your hard drive) you create under Windows Vista must have a file system associated with it.

When selecting a file system, you can select FAT32 or NTFS. You typically select file systems based on the features you want to use and whether you will need to access the file system using other operating systems. If you have a FAT32 partition and want to update it to NTFS,

you can use the Convert utility. The features of each file system and the procedure for converting file systems are covered in the following sections.

File System Selection

Your file system is used to store and retrieve the files stored on your hard drive. One of the most fundamental choices associated with file management is the choice of your file system's configuration. As explained in Chapter 1, "Getting Started with Windows Vista," Windows Vista supports the FAT32 and NTFS file systems. It is recommended that you use NTFS with Windows Vista, since doing so will allow you to take advantage of features such as local security, file compression, and file encryption. You should choose FAT32 if you want to dual-boot your computer with a version of Windows that does not support NTFS, because these file systems are backward compatible with other operating systems.

Table 7.1 summarizes the capabilities of each file system, and they are described in more detail in the following sections.

TABLE 7.1 File System Capabilities

Feature	FAT16	FAT32	NTFS
Supporting operating systems	Most	Windows 95 OSR2, Windows 98, Windows Me, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista	Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista
Long filename support	Yes	Yes	Yes
Efficient use of disk space	No	Yes	Yes
Compression support	No	No	Yes
Encryption support	No	No	Yes
Support for local security	No	No	Yes
Support for network security	Yes	Yes	Yes
Maximum volume size	2GB	32GB	16TB with 4KB clusters or 256TB with 64KB clusters

Windows Vista also supports *Compact Disk File System (CDFS)*. However, CDFS cannot be managed. It is used only to mount and read CDs.

FAT16

FAT16 was first used with DOS (Disk Operating System) 3.0 in 1981. With FAT16, the directory-entry table keeps track of the location of the file's first block, the filename and extension, the date- and timestamps on the file, and any attributes associated with the file. FAT16 is similar in nature to a card catalog at a library—when the operating system needs a file, the FAT listing is consulted.

The main advantage of FAT16 is that almost all operating systems support this file system. This makes FAT16 a good choice if the computer will dual-boot with other operating systems (see Chapter 1 for more information about dual-booting). FAT16 is also a good choice for small partitions (FAT16 partitions can be only up to 2GB in size). Because FAT16 is a very simple file system, the overhead associated with storing files is much smaller than with NTFS.

The problem with using FAT16 is that it was designed to be used as a single-user file system, and thus it does not support any kind of security. Prior to Windows 95, FAT16 did not support long filenames. Other file systems, such as NTFS, offer many more features, including local security, file compression, and encrypting capabilities.

FAT32

FAT32 is an updated version of FAT. FAT32 was first shipped with Windows 95 OSR2 (Operating System Release 2), and can be used by Windows Vista.

One of the main advantages of FAT32 is its support for smaller cluster sizes, which results in more efficient space allocation than was possible with FAT16. Files stored on a FAT32 partition can use 20 to 30 percent less disk space than files stored on a FAT16 partition. FAT32 supports drive sizes from 512MB up to 2TB, although if you create and format a FAT32 partition through Windows Vista, the FAT32 partition can only be up to 32GB. Because of the smaller cluster sizes, FAT32 can also load programs up to 50 percent faster than programs loaded from FAT16 partitions.

The main disadvantages of FAT32 compared to NTFS are that it does not provide as much support for larger hard drives and it does not provide very robust security options. It also offers no native support for disk compression.

NTFS

NTFS, which was first used with the NT operating system, offers the highest level of service and features for Windows Vista computers. NTFS partitions can be up to 16TB with 4KB clusters or 256TB with 64KB clusters.

NTFS offers comprehensive folder- and file-level security. This allows you to set an additional level of security for users who access the files and folders locally or through the

network. For example, two users who share the same Windows Vista computer can be assigned different NTFS permissions, so that one user has access to a folder but the other user is denied access to that folder.

NTFS also offers disk-management features—such as compression and encryption services—and data recovery features. The disk-management features are covered later in this chapter. The data-recovery features are covered in Chapter 11, "Maintaining and Optimizing Windows Vista."

You should also be aware that there are several different versions of NTFS. Every version of Windows 2000 uses NTFS 3.0. Windows Vista, Windows XP, and Windows Server 2003 use NTFS 3.1. NTFS versions 3.0 and 3.1 use similar disk formats, so Windows 2000 computers can access NTFS 3.1 volumes and Windows Vista computers can access NTFS 3.0 volumes. The features of NTFS 3.1 include the following:

- When files are read or written to a disk, they can be automatically encrypted and decrypted.
- Reparse points are used with mount points to redirect data as it is written or read from a folder to another volume or physical disk.
- There is support for sparse files, which is used by programs that create large files but allocate disk space only as needed.
- Remote storage allows you to extend your disk space by making removable media (for example, external tapes) more accessible.
- You can use recovery logging on NTFS metadata, which is used for data recovery when a power failure or system problem occurs.

File System Conversion

In Windows Vista, you can convert FAT32 partitions to NTFS. File system conversion is the process of converting one file system to another without the loss of data. If you format a drive as another file system, as opposed to converting that drive, all the data on that drive will be lost.

To convert a partition, you use the *Convert* command-line utility. The syntax for the `Convert` command is as follows:

```
Convert [drive:] /fs:ntfs
```

For example, if you wanted to convert your D: drive to NTFS, you would type the following from a command prompt:

```
Convert D: /fs:ntfs
```

When the conversion process begins, it will attempt to lock the partition. If the partition cannot be locked—perhaps because the partition contains the Windows Vista operating system files or the system's page file—the conversion will not take place until the computer is restarted.

You can use the `/v` switch with the `Convert` command. This switch specifies that you want to use verbose mode, and all messages will be displayed during the conversion process. You can also use the `/NoSecurity` switch, which specifies that all converted files and folders will have no security applied by default so they can be accessed by anyone.

In Exercise 7.1, you will convert your D: drive from FAT32 to NTFS. This exercise assumes that you have a D: drive that is formatted with the FAT32 file system.

EXERCISE 7.1

Converting a FAT32 Partition to NTFS

1. Copy some folders to the D: drive.
2. Select Start, then type **cmd** into the Search box to open a command prompt.
3. In the Command Prompt dialog box, type **`Convert D: /fs:ntfs`** and press Enter.
4. After the conversion process is complete, close the Command Prompt dialog box.
5. Verify that the folders you copied in step 1 still exist on the partition.

If you choose to convert a partition from FAT32 to NTFS, and the conversion has not yet taken place, you can cancel the conversion by editing the Registry with the `REGEDIT` command. The key that needs to be edited is `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager`. The `BootExecute` value needs to be changed from `autoconv \DosDevices\x: /FS:NTFS` to `autocheck autochk*`.

Configuring Disk Storage

Windows Vista supports two types of disk storage: basic and dynamic. Basic storage is backward compatible with other operating systems and can be configured to support up to four partitions. Dynamic storage is supported by Windows 2000, Windows XP, Windows Server 2003, and Windows Vista, and allows storage to be configured as volumes. The following sections describe the basic storage and dynamic storage configurations.

Basic Storage

Basic storage consists of primary and extended partitions and logical drives. The first partition that is created on a hard drive is called a *primary partition* and is usually represented as drive C:. Primary partitions use all of the space that is allocated to the partition and use a single drive letter to represent the partition. Each physical drive can have up to four partitions. You can set up four primary partitions, or you can have three primary partitions and one extended partition. With an *extended partition*, you can allocate the space however you like, and each sub-allocation of space (called a *logical drive*) is represented by a different drive letter. For example, a 500MB extended partition could have a 250MB D: partition and a 250MB E: partition.

At the highest level of disk organization, you have a physical hard drive. You cannot use space on the physical drive until you have logically partitioned the physical drive. A *partition* is a logical definition of hard drive space.

One of the advantages of using multiple partitions on a single physical hard drive is that each partition can have a different file system. For example, the C: drive might be FAT32 and the D: drive might be NTFS. Multiple partitions also make it easier to manage security requirements.

Laptop computers support only basic storage.

Dynamic Storage

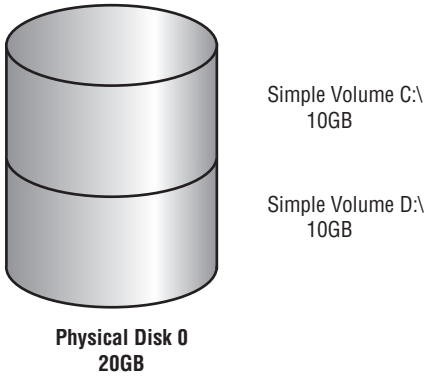
Dynamic storage is a Windows Vista feature that consists of a *dynamic disk* divided into dynamic *volumes*. Dynamic volumes cannot contain partitions or logical drives.

Dynamic storage supports three dynamic volume types: simple volumes, spanned volumes, and striped volumes. To set up dynamic storage, you create or upgrade a basic disk to a dynamic disk. Then you create dynamic volumes within the dynamic disk. You create dynamic storage with the Windows Vista Disk Management utility, which is discussed after the descriptions of the dynamic volume types.

Simple Volumes

A *simple volume* contains space from a single dynamic drive. The space from the single drive can be contiguous or noncontiguous. Simple volumes are used when you have enough disk space on a single drive to hold your entire volume. Figure 7.1 illustrates two simple volumes on a physical disk.

FIGURE 7.1 Two simple volumes



Spanned Volumes

A *spanned volume* consists of disk space on two or more dynamic drives; up to 32 dynamic drives can be used in a spanned volume configuration. Spanned volume sets are used to dynamically increase the size of a dynamic volume. When you create spanned volumes, the data is written sequentially, filling space on one physical drive before writing to space on the next physical drive in the spanned volume set. Typically, administrators use spanned volumes when they are running out of disk space on a volume and want to dynamically extend the volume with space from another hard drive.

You do not need to allocate the same amount of space to the volume set on each physical drive. This means you could combine a 500MB partition on one physical drive with two 750MB partitions on other dynamic drives, as shown in Figure 7.2.

Because data is written sequentially, you do not see any performance enhancements with spanned volumes as you do with striped volumes (which we discuss next). The main disadvantage of spanned volumes is that if any drive in the spanned volume set fails, you lose access to all of the data in the spanned set.

Striped Volumes

A *striped volume* stores data in equal stripes between two or more (up to 32) dynamic drives, as illustrated in Figure 7.3. Since the data is written sequentially in the stripes, you can take advantage of multiple I/O performance and increase the speed at which data reads and writes take place. Typically, administrators use striped volumes when they want to combine the space of several physical drives into a single logical volume and increase disk performance.

The main disadvantage of striped volumes is that if any drive in the striped volume set fails, you lose access to all of the data in the striped set.

Mirrored volumes and RAID-5 volumes are fault-tolerant dynamic disk configurations. These options are available only with Windows 2000 Server and Windows Server 2003.

If you created a multidisk volume—such as a spanned, mirrored, or striped set, or a striped set with parity—with Windows NT 4 or earlier, it is not supported by Windows Vista or Windows Server 2003.

FIGURE 7.2 A spanned volume set

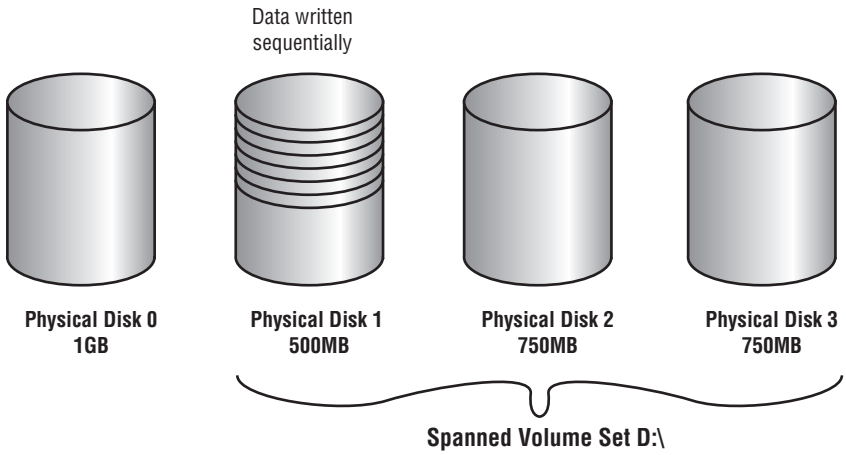
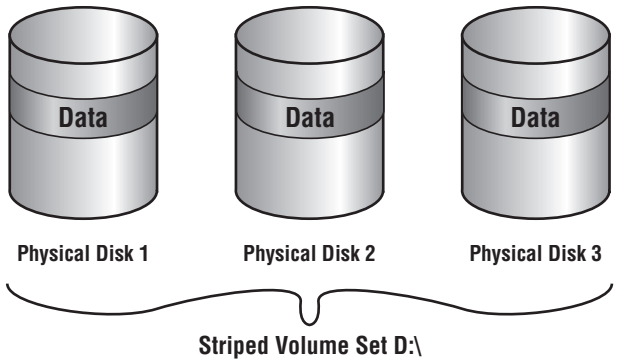


FIGURE 7.3 A striped volume set



Using the Disk Management Utility

The *Disk Management utility* is a graphical tool for managing disks and volumes within Windows Vista. In this section, you will learn how to access the Disk Management utility and use it to manage basic tasks, basic storage, and dynamic storage. You will also learn about troubleshooting disks through disk status codes.

To have full permissions to use the Disk Management utility, you must be logged on with Administrative privileges. To access the utility, right-click Computer from the Start Menu and select Manage, and then in Computer Management, select Disk Management. You could also use Control Panel ➢ System and Maintenance ➢ Administrative Tools ➢ Computer Management. Expand the Storage folder to see the Disk Management utility. The Disk Management utility's opening window, shown in Figure 7.4, shows the following information:

- The volumes that are recognized by the computer
- The type of disk, either basic or dynamic
- The type of file system used by each partition
- The status of the partition and whether the partition contains the system or boot partition
- The capacity (amount of space) allocated to the partition
- The amount of free space remaining on the partition
- The amount of overhead associated with the partition

Windows Vista includes a command-line utility called Diskpart, which can be used as a command-line alternative to the Disk Management utility. You can view all of the options associated with the Diskpart utility by typing **Diskpart** at a command prompt, and then typing **?** at the Diskpart prompt.

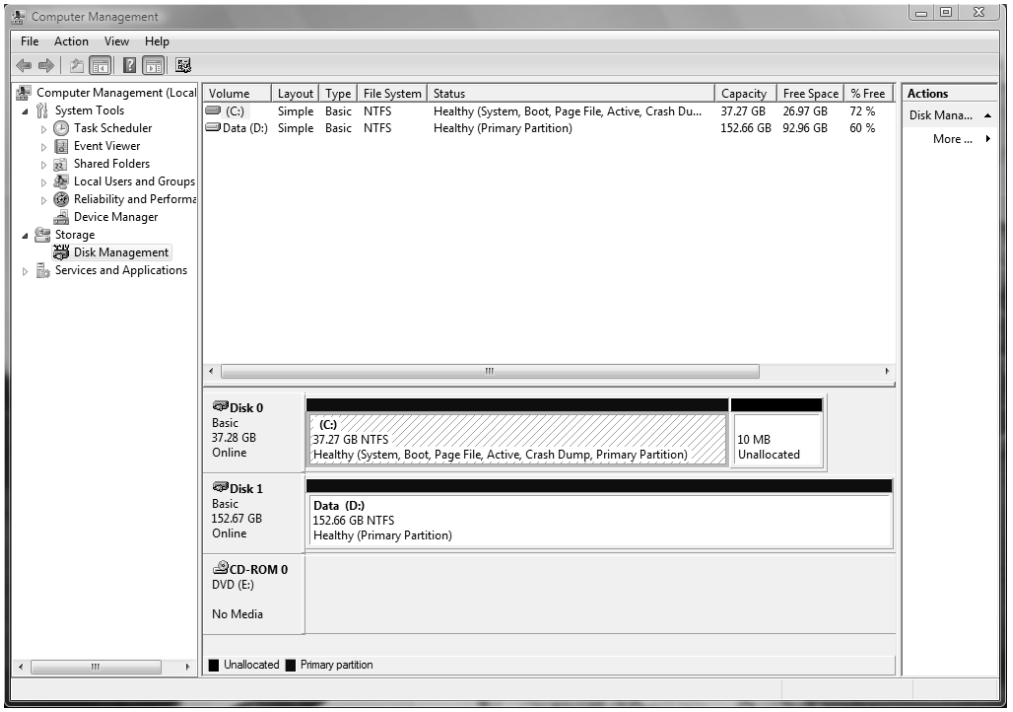
You can also add Disk Management as a Microsoft Management Console (MMC) snap-in, as described in Chapter 3, "Configuring the Windows Vista Environment."

Managing Basic Tasks

With the Disk Management utility, you can perform a variety of basic tasks. These tasks are discussed in the sections that follow:

- View disk properties.
- View volume and local disk properties.
- Add a new disk.
- Create partitions and volumes.

FIGURE 7.4 The Disk Management window



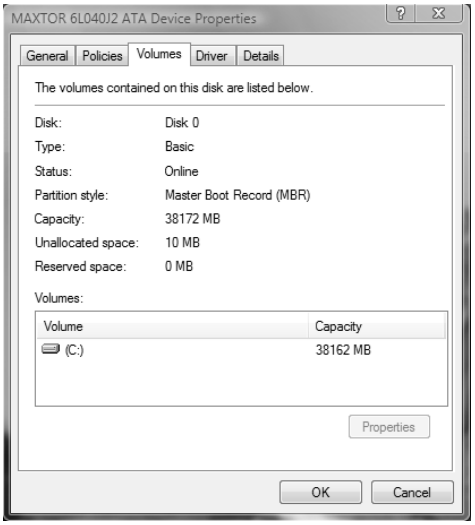
- Upgrade a basic disk to a dynamic disk.
- Change a drive letter and path.
- Delete partitions and volumes.

Viewing Disk Properties

To view the properties of a disk, right-click the disk number in the lower panel of the Disk Management main window (see Figure 7.4) and choose Properties from the context menu. This brings up the disk's Properties dialog box. Click the Volumes tab to see the volumes associated with the disk, as shown in Figure 7.5, which contains the following disk properties:

- The disk number
- The type of disk (basic, dynamic, CD-ROM, removable, DVD, or unknown)
- The status of the disk (online or offline)
- The capacity of the disk
- The amount of unallocated space on the disk
- The logical volumes that have been defined on the physical drive

FIGURE 7.5 The Volumes tab of a disk's Properties dialog box



If you click the General tab of a disk's Properties dialog box, the hardware device type, the hardware vendor that produced the drive, the physical location of the drive, and the device status are displayed.

Viewing Volume and Local Disk Properties

On a dynamic disk, you manage volume properties. On a basic disk, you manage local disk properties. Volumes and local disks perform the same function, and the options discussed in the following sections apply to both. (The examples here are based on a dynamic disk using a simple volume. If you are using basic storage, you will view the local disk properties rather than the volume properties.)

To see the properties of a volume, right-click the volume in the upper panel of the Disk Management main window and choose Properties. This brings up the volume's Properties dialog box. Volume properties are organized on six tabs: General, Tools, Hardware, Sharing, Security, and Previous Versions. The Security tab appears only for NTFS volumes. All these tabs are covered in detail in the following sections.

General

The information on the General tab of the volume's Properties dialog box, as seen in Figure 7.6, gives you a general idea of how the volume is configured. This dialog box shows the label, type, file system, used and free space, and capacity of the volume. The label is shown in an editable

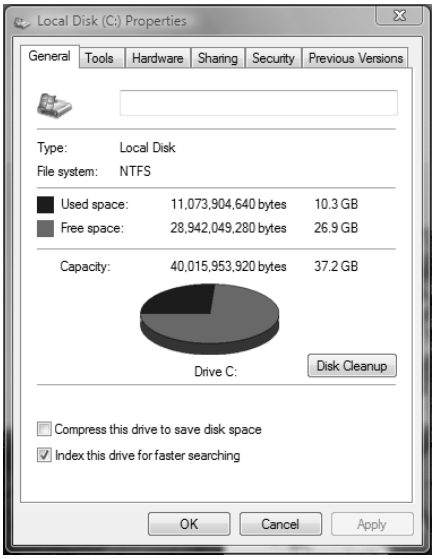
text box, and you can change it if desired. The space allocated to the volume is shown in a graphical representation as well as in text form.

The label on a volume or local disk is for informational purposes only. For example, depending on its use, you might give a volume a label such as APPS or ACCTDB.

The Disk Cleanup button starts the Disk Cleanup utility, with which you can delete unnecessary files and free disk space. This utility is discussed later in this chapter in the "Using the Disk Cleanup Utility" section.

This tab also allows you to configure compression for the volume and to indicate whether the volume should be indexed.

FIGURE 7.6 General properties for a volume



Tools

The Tools tab of the volume's Properties dialog box, shown in Figure 7.7, provides access to three tools:

- Click the Check Now button to run the Check Disk utility to check the volume for errors. You would do this if you were experiencing problems accessing the volume or if the volume had been open during a system restart that did not go through a proper shutdown sequence. This utility is covered in more detail in "Troubleshooting Disk Devices and Volumes" later in this chapter.

- Click the Defragment Now button to run the Disk Defragmenter utility. This utility defragments files on the volume by storing the files contiguously on the hard drive. Defragmentation is discussed later in this chapter, in the "Using the Disk Defragmenter Utility" section.
- Click the Backup Now button to open the Backup Status and Configuration dialog box, which allows you to configure backup procedures.

Hardware

The Hardware tab of the volume's Properties dialog box, shown in Figure 7.8, lists the hardware associated with the disk drives that are recognized by the Windows Vista operating system. The bottom half of the dialog box shows the properties of the device that is highlighted in the top half of the dialog box.

For more details about a hardware item, highlight it and click the Properties button in the lower-right corner of the dialog box. This brings up a Properties dialog box for the item (for example, Figure 7.9). With luck, your Device Status field will report that "This device is working properly." If that's not the case, you can click the Troubleshoot button to get a troubleshooting wizard that will help you discover what the problem is.

Sharing

On the Sharing tab of the volume's Properties dialog box, shown in Figure 7.10, you can specify whether or not the volume is shared. Volumes are not shared by default. To share a volume, you can click the Advanced Sharing button, which will allow you to specify whether the volume is shared and, if so, what the name of the share should be. You will also be able to specify who will have access to the shared volume.

FIGURE 7.7 The Tools tab of the volume's Properties dialog box

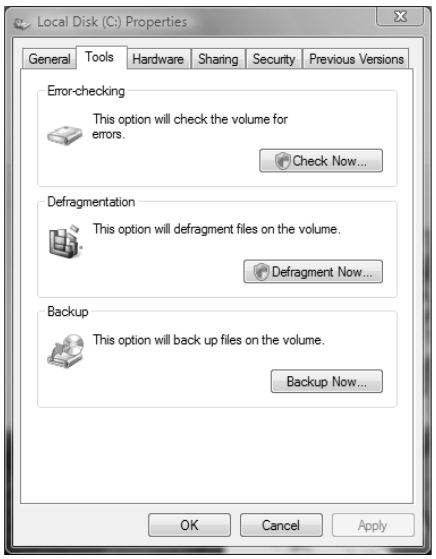


FIGURE 7.8 The Hardware tab of the volume's Properties dialog box

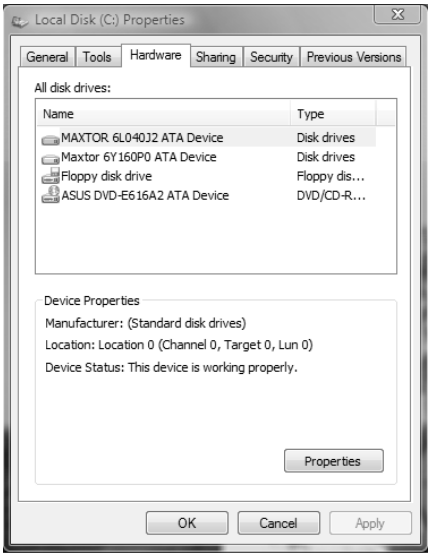


FIGURE 7.9 A disk drive's Properties dialog box, accessed through the Hardware tab of the volume's Properties dialog box

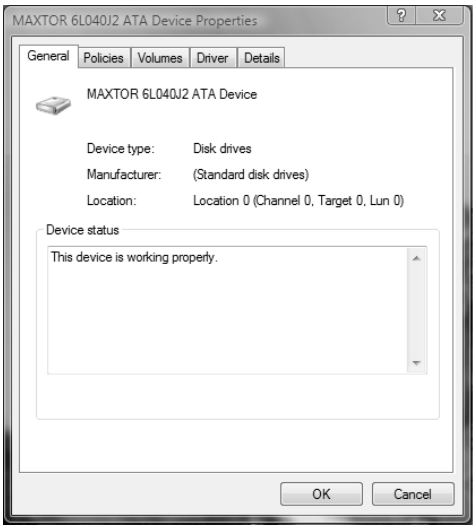


FIGURE 7.10 The Sharing tab of the volume's Properties dialog box

Security

The Security tab of the volume's Properties dialog box, shown in Figure 7.11, appears only for NTFS volumes. The Security tab is used to set the NTFS permissions for the volume.

Previous Versions

The Previous Versions tab displays shadow copies of the files that are created by System Restore, as shown in Figure 7.12. Shadow copies of files are backup copies created by Windows in the background in order to allow you to restore the system to a previous state. On the Previous Versions tab, you can select a copy of the volume and either view the contents of the shadow copy or copy the shadow copy to another location. If System Restore is not enabled, then shadow copies of a volume will not be created.

Adding a New Disk

New hard disks can be added to a system in order to increase the amount of disk storage you have. This is a fairly common task that you will need to perform as your application programs and files grow larger. How you add a disk depends on whether your computer supports hot swapping of drives. *Hot swapping* is the process of adding a new hard drive while the computer is turned on. Most desktop computers do not support this capability.

FIGURE 7.11 The Security tab of the volume's Properties dialog box

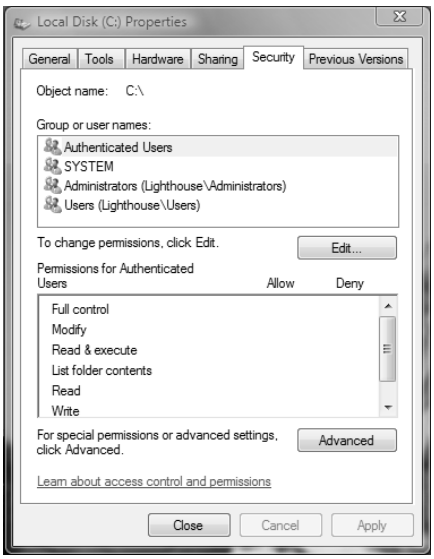
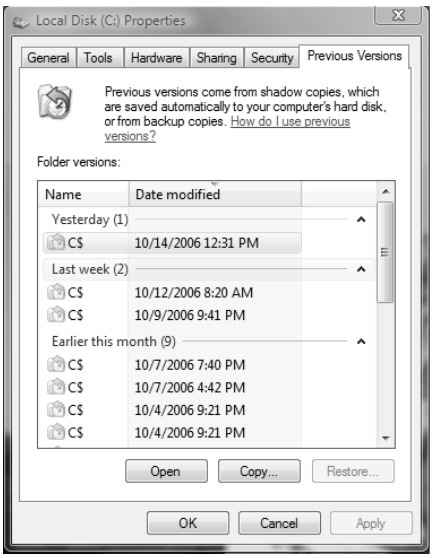


FIGURE 7.12 The Previous Versions tab of the volume's Properties dialog box



The following list specifies configuration options:

Computer doesn't support hot swapping If your computer does not support hot swapping, you must first shut down the computer before you add a new disk. Then add the drive according to the manufacturer's directions. When you've finished, restart the computer. You should find the new drive listed in the Disk Management utility.

Computer supports hot swapping If your computer does support hot swapping, you don't need to turn off your computer first. Just add the drive according to the manufacturer's directions. Then open the Disk Management utility and select Action ➢ Rescan Disks. You should find the new drive listed in the Disk Management utility.

Your user account must be a member of the Administrators group in order to install a new drive.

Creating Partitions and Volumes

Once you add a new disk, the next step is to create a partition (on a basic disk) or a volume (on a dynamic disk). Partitions and volumes fill similar roles in the storage of data on disks, and the processes for creating them are the same.

Creating a Volume or a Partition

The New Volume Wizard guides you through the process of creating a new volume, as follows:

1. In the Disk Management utility, right-click an area of free storage space and choose the type of volume to create. If only one drive is installed, you will only be able to create a simple volume. You can click New Simple Volume to create a new simple volume.
2. The Welcome to the New Simple Volume Wizard appears. Click the Next button to continue.
3. The Select Volume Size screen appears, as shown in Figure 7.13. Select the size of volume to create, and then click Next to continue.
4. Next you see the Assign Drive Letter or Path screen, as shown in Figure 7.14. You can specify a drive letter, mount the volume as an empty folder, or choose not to assign a drive letter or drive path. If you choose to mount the volume as an empty folder, you can have an unlimited number of volumes, negating the drive-letter limitation. Make your selections, and click Next to continue.

If you choose not to assign a drive letter or path, users will not be able to access the volume.

FIGURE 7.13 The Select Volume Size screen

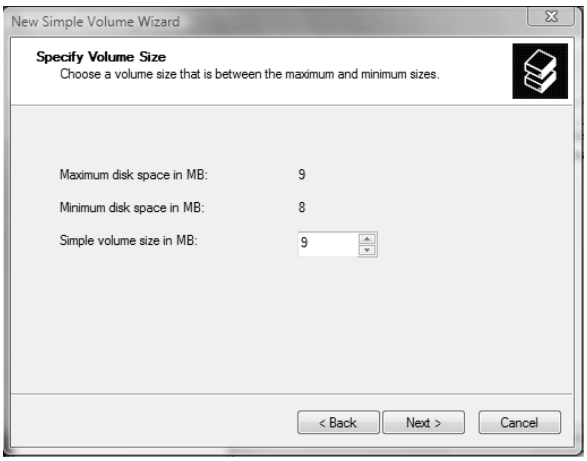


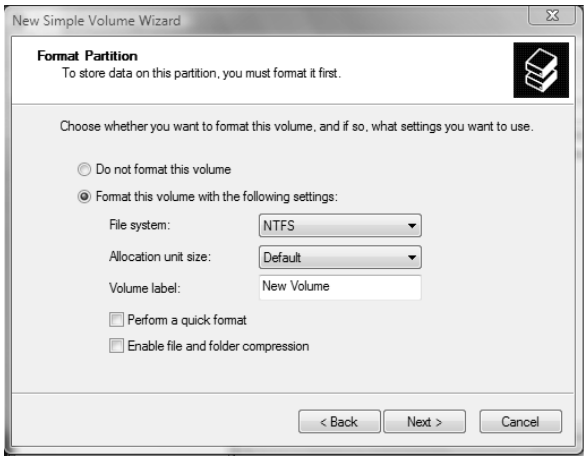
FIGURE 7.14 The Assign Drive Letter or Path screen

5. The Format Partition screen appears, as shown in Figure 7.15. This screen allows you to choose whether you will format the volume. If you choose to format the volume, you can format it as FAT, FAT32, or NTFS. You can also select the allocation block size, enter a volume label (for information only), specify a quick format, or choose to enable file and folder compression. After you've made your choices, click Next.

Specifying a quick format is risky because this format does not scan the disk for bad sectors, which is done in a normal format operation.

6. The Completing the New Volume Wizard screen appears next. Verify your selections. If you need to change any of them, click the Back button to reach the appropriate screen. When everything is correctly set, click the Finish button.

FIGURE 7.15 The Format Partition screen



In Exercise 7.2, you will create a volume from the free space that was left on your drive when you installed Windows Vista (in Exercise 1.1), as specified in Chapter 1.

EXERCISE 7.2

Creating a New Volume

1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools. Double-click Computer Management; then expand Storage and then Disk Management.
2. Right-click an area of free storage and select the New Simple Volume option.
3. The New Simple Volume Wizard starts. Click Next to continue.
4. The Select Volume Size screen appears. Specify a partition size of 250MB and click Next.
5. The Assign Drive Letter or Path screen appears. Click Next to assign the default drive letter shown on this screen. If you are using the recommended configuration, C: and D: are assigned as drive letters, E: should be your CD-ROM drive, and the next available drive will be F:.

EXERCISE 7.2 *(continued)*

6. In the Format Partition screen, choose to format the drive as NTFS and leave the other settings at their default values. Click Next.
7. The Completing the New Volume Wizard screen appears. Click the Finish button.

Upgrading a Basic Disk to a Dynamic Disk

When you install a fresh installation of Windows Vista, your drives are configured as basic disks. To take advantage of the features offered by Windows Vista dynamic disks, you must upgrade your basic disks to dynamic disks.

Upgrading basic disks to dynamic disks is a one-way process as far as preserving data is concerned and a potentially dangerous operation. Before you perform this upgrade (or make any major change to your drives or volumes), create a new backup of the drive or volume and verify that you can successfully restore the backup.

The following steps are involved in the disk-upgrade process:

1. In the Disk Management utility, right-click the disk you want to convert, and select the Convert to Dynamic Disk option.
2. In the Convert to Dynamic Disk dialog box, check the disk that you want to upgrade and click OK.
3. In the Disks to Convert dialog box, click the Convert button.
4. A confirmation dialog box warns you that you will no longer be able to boot previous versions of Windows from this disk. Click the Yes button to continue to convert the disk.

Changing the Drive Letter and Path

Suppose that you have drive C: assigned as your first partition and drive D: assigned as your CD drive. You add a new drive and partition it as a new volume. By default, the new partition is assigned as drive E:. If you want your logical drives to appear listed before the CD drive, you can use the Disk Management utility's Change Drive Letter and Paths option to rearrange your drive letters.

When you need to reassign drive letters, right-click the volume for which you want to change the drive letter and choose Change Drive Letter and Paths. This brings up the dialog box shown in Figure 7.16. Click the Change button to access the Change Drive Letter or Path dialog box (Figure 7.17). Use the drop-down list next to the Assign the Following Drive Letter option to select the drive letter you want to assign to the volume.

In Exercise 7.3, you will edit the drive letter of the partition you created in Exercise 7.2.

FIGURE 7.16 The dialog box for changing a drive letter or path

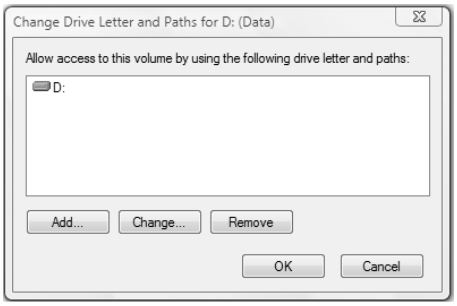
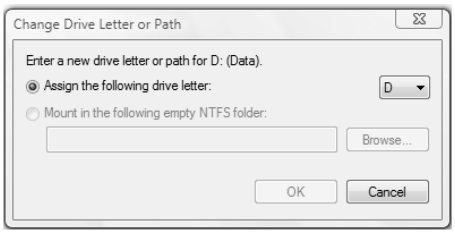


FIGURE 7.17 Editing the drive letter



EXERCISE 7.3

Editing a Drive Letter

1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools. Double-click Computer Management; then expand Storage and then Disk Management.
2. Right-click the drive you created in Exercise 7.2 and select Change Drive Letter and Paths.
3. In the Change Drive Letter and Paths dialog box, click the Change button.
4. In the Change Drive Letter or Path dialog box, select a new drive letter and click OK.
5. In the dialog box that appears, click the Yes button to confirm that you want to change the drive letter.

Deleting Partitions and Volumes

You might delete a partition or volume if you wanted to reorganize your disk or to make sure that data would not be accessed.

Once you delete a partition or volume, it is gone forever.

To delete a partition or volume, in the Disk Management window right-click the partition or volume and choose the Delete Volume option. You will see a warning that all the data on the partition or volume will be lost. Click Yes to confirm that you want to delete the volume or partition.

The system volume, the boot volume, or any volume that contains the active paging (swap) file can't be deleted through the Disk Management utility. If you are trying to remove these partitions because you want to delete Windows Vista, you can use a third-party disk-management utility, such as Partition Magic.

Managing Basic Storage

The Disk Management utility offers limited support for managing basic storage. You can create, delete, and format partitions on basic drives. You can also extend or shrink volumes on basic disks. Additionally, you can delete volume sets and striped sets. Most other disk-management tasks require that you upgrade your drive to dynamic disks. (The upgrade process was described in the earlier section, "Upgrading a Basic Disk to a Dynamic Disk.")

Managing Dynamic Storage

As noted earlier in this chapter, a dynamic disk can contain simple, spanned, or striped volumes. Through the Disk Management utility, you can create volumes of each type. You can also create an extended volume, which is the process of adding disk space to a single simple volume. The following sections describe these disk-management tasks.

Creating Simple, Spanned, and Striped Volumes

As explained earlier in "Creating Partitions and Volumes," you use the New Volume Wizard to create a new volume. To start the wizard, in the Disk Management utility right-click an area of free space where you want to create the volume. Then, you can choose the type of volume you want to create: Simple, Spanned, or Striped.

When you choose to create a spanned volume, you are creating a new volume from scratch that includes space from two or more physical drives, up to a maximum of 32 drives.

When you choose to create a striped volume, you are creating a new volume that combines free space from two to 32 drives into a single logical partition. The free space on all drives must be equal in size. Data in the striped volume is written across all drives in 64KB stripes. (Data in spanned and extended volumes is written sequentially.)

Creating Extended Volumes

When you create an extended volume, you are taking a single, simple volume (maybe one that is almost out of disk space) and adding more disk space to it, using free space that exists on the same physical hard drive. When the volume is extended, it is seen as a single drive letter. To extend a volume, the simple volume must be formatted as NTFS. You cannot extend a system or boot partition.

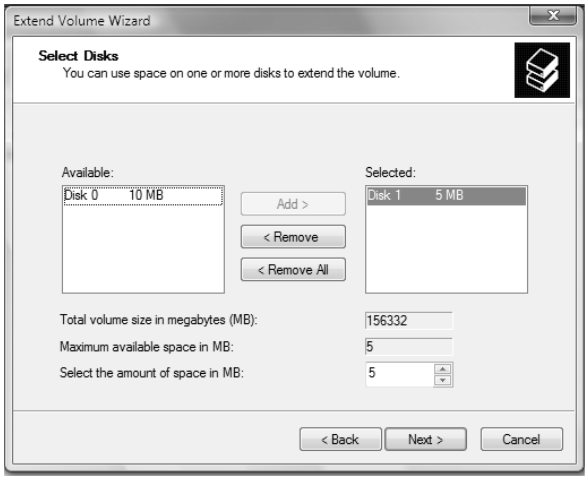
An extended volume assumes that you are using only one physical drive. A spanned volume assumes that you are using two or more physical drives.

Here are the steps to create an extended volume:

1. In the Disk Management utility, right-click the volume you want to extend and choose Extend Volume.
2. The Extend Volume Wizard starts. Click Next.
3. The Select Disks screen appears, as shown in Figure 7.18. You can specify the maximum size of the extended volume. The maximum size you can specify is determined by the amount of free space that exists in all of the dynamic drives on your computer. Click Next to continue.
4. The Completing the Extend Volume Wizard screen appears. Click the Finish button.

Once a volume is extended, no portion of the volume can be deleted without losing data on the entire set. (However, you can shrink a volume without losing data by using the Shrink Volume option in Disk Management.)

FIGURE 7.18 The Select Disks screen



Real World Scenario

You're Running Out of Disk Space

Martha, a user on your network, is running out of disk space. The situation needs to be corrected so she can be brought back up and running as quickly as possible. Martha has a 40GB drive (C:) that runs a very large customer database. She needs additional space added to the C: drive so the database will recognize the data, since it must be stored on a single drive letter. Martha's computer has a single IDE drive with nothing attached to the second IDE channel.

You have two basic options for managing space in these circumstances. One is to upgrade the disk to a larger disk, but this will necessitate reinstalling the OS and the applications and restoring the user's data. The other choice is to add a temporary second drive and extend the volume. This will at least allow Martha to be up and running—but it should not be considered a permanent solution. If you do choose to extend the volume, and then either drive within the volume set fails, the user will lose access to both drives. When Martha's workload allows time for maintenance, you can replace the volume set with a single drive.

Troubleshooting Disk Management

The Disk Management utility can be used to troubleshoot disk errors through a set of status codes; however, if a disk will not initialize, no status code will be displayed. Disks will not initialize if there is no valid disk signature.

Using Disk Management Status Codes

The main window of the Disk Management utility displays the status of disks and volumes. The following list contains the possible status codes and a description of each code; these are very useful in troubleshooting disk problems.

Online Indicates that the disk is accessible and that it is functioning properly. This is the normal disk status.

Online (Errors) Only used with dynamic disks. Indicates that I/O errors have been detected on the dynamic disk. One possible fix for this error is to right-click the disk and select Reactivate Disk to attempt to return the disk to Online status. This fix will work only if the I/O errors were temporary. You should immediately back up your data if you see this error and suspect that the I/O errors are not temporary.

Healthy Specifies that the volume is accessible and functioning properly.

Healthy (At Risk) Used to indicate that a dynamic volume is currently accessible, but I/O errors have been detected on the underlying dynamic disk. This option is usually associated with Online (Errors) for the underlying disk.

Offline or Missing Used only with dynamic disks. Indicates that the disk is not accessible. This can occur if the disk is corrupted or the hardware has failed. If the error is not caused by

hardware failure or major corruption, you may be able to re-access the disk by using the Reactivate Disk option to return the disk to Online status. If the disk was originally offline and then the status changed to Missing, it indicates that the disk has become corrupted, has been powered down, or was disconnected.

Unreadable This can occur on basic or dynamic disks. Indicates that the disk is inaccessible and might have encountered hardware errors, corruption, or I/O errors or that the system disk configuration database is corrupted. This message may also appear when a disk is spinning up while the Disk Management utility is rescanning the disks on the computer.

Failed Can be seen with basic or dynamic volumes. Specifies that the volume can't be started. This can occur because the disk is damaged or the file system is corrupted. If this message occurs with a basic volume, you should check the underlying disk hardware. If the error occurs on a dynamic volume, verify that the underlying disks are Online.

Unknown Used with basic and dynamic volumes. Occurs if the boot sector for the volume becomes corrupted—for example, from a virus. This error can also occur if no disk signature is created for the volume.

Incomplete Occurs when you move some, but not all, of the disks from a multidisk volume. If you do not complete the multivolume set, then the data will be inaccessible.

Foreign Can occur if you move a dynamic disk from a computer running Windows 2000 (any version), Windows XP Professional, or Windows Server 2003 to a Windows Vista computer. This error is caused because configuration data is unique to computers where the dynamic disk was created. You can correct this error by right-clicking the disk and selecting the option Import Foreign Disks. Any existing volume information will then be visible and accessible.

Troubleshooting Disks That Fail to Initialize

When you add a new disk to your computer in Windows Vista, the disk does not initially contain a disk signature, which is required for the disk to be recognized by Windows. Disk signatures are at the end of the sector marker on the Master Boot Record (MBR) of the drive. When you install a new drive and run the Disk Management utility, a wizard starts and lists all new disks that have been detected. The disk signature is written through this process. If you cancel the wizard before the disk signature is written, you will see the disk status Not Initialized. To initialize a disk, you right-click the disk you want to initialize and select the Initialize Disk option.

Managing Data Compression

Data compression is the process of storing data in a form that takes less space than does uncompressed data. If you have ever "zipped" or "packed" a file, you have used data compression. With Windows Vista, data compression is available only on NTFS partitions. The compression algorithms support cluster sizes only up to 4KB, so if you are using larger cluster sizes, NTFS compression support is not available. If you have the Modify permission on an NTFS volume, you can manage data compression through Windows Explorer or the Compact command-line utility.

Files as well as folders in the NTFS file system can be either compressed or uncompressed. Files and folders are managed independently, which means that a compressed folder can contain uncompressed files, and an uncompressed folder can contain compressed files.

Access to compressed files by applications is transparent. For example, if you access a compressed file through Microsoft Word, the file will be uncompressed automatically when it is opened and then automatically compressed again when it is closed.

Data compression is available only on NTFS partitions. If you copy or move a compressed folder or file to a FAT partition, Windows Vista automatically uncompresses the folder or file.

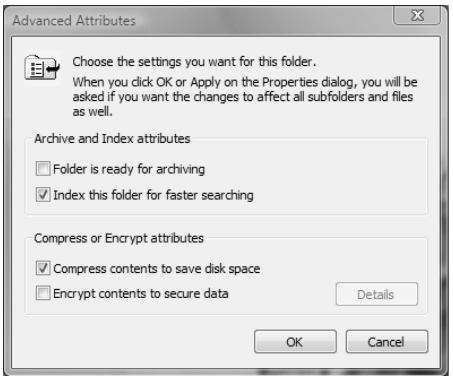
Windows Vista does not allow you to have a folder or file compressed and encrypted at the same time. A feature included with Windows Server 2003 is support for concurrent compression and encryption. Encryption is discussed in the "Managing Data Encryption with EFS" section later in this chapter.

In Exercise 7.4, you will compress and uncompress folders and files. This exercise assumes that you have completed Exercise 7.1.

EXERCISE 7.4

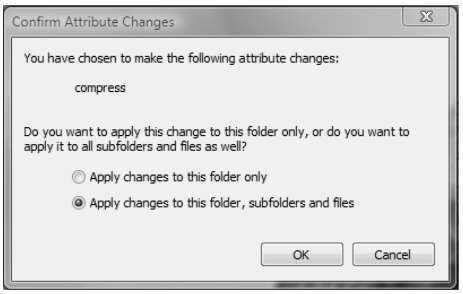
Compressing and Uncompressing Folders and Files

1. Select Start ➢ Run, and then type **Explorer** and click OK.
2. In Windows Explorer, find and select Computer, the Local Disk (D:), and then a folder on the D: drive. The folder you select should contain files.
3. Right-click the folder and select Properties. In the General tab of the folder's Properties dialog box, note the value listed for Size on Disk. Then click the Advanced button.
4. In the Advanced Attributes dialog box, check the Compress Contents to Save Disk Space option. Then click OK.



EXERCISE 7.4 *(continued)*

5. In the Confirm Attribute Changes dialog box, select the option Apply Changes to This Folder, Subfolders and Files. (If this confirmation dialog box does not appear, you can display it by clicking the Apply button in the Properties dialog box.) Click OK to confirm your changes.



6. On the General tab of the folder's Properties dialog box, note the value that now appears for Size on Disk. This size should have decreased because you compressed the folder.

To uncompress folders and files, repeat the steps of this exercise and uncheck the Compress Contents to Save Disk Space option in the Advanced Attributes dialog box.

You can specify that compressed files be displayed in a different color from the uncompressed files. To do so, in Windows Explorer, select Organize ➢ Folder and Search Options ➢ View. Under Files and Folders, check the Show Encrypted or Compressed NTFS Files in Color option.

Using the Compact Command-Line Utility

The command-line options for managing file and folder compression are `Compact` and `Expand`. You can access these commands from a command prompt. Using the `Compact` command offers you more control over file and folder compression than Windows Explorer. For example, you can use the `Compact` command with a batch script or to compress only files that meet a specific criterion (for example, all the `.doc` files in a specific folder).

The options that can be used with the `Compact` command are as follows:

- `/C`—Compresses the specified file or folder
- `/U`—Uncompresses the specified file or folder
- `/S:dir`—Used to specify which folder should be compressed or uncompressed

- /A—Displays any files that have hidden or system file attributes
- /I—Indicates that any errors should be ignored
- /F—Forces a file to be compressed
- /Q—Used with reporting, to report only critical information
- /?—Displays help

Using Compressed (Zipped) Folders

Windows Vista also supports compressed (zipped) folders. This feature is different from NTFS compressed folders. The advantage of using compressed (zipped) folders is that it is supported on FAT or NTFS volumes. In addition, you can use compressed (zipped) folders to share data with other programs that use zipped files.

Within Windows Explorer you create a zipped folder (or file) by right-clicking on a folder and selecting Send To ➢ Compressed (Zipped) Folder. You create a zipped file by right-clicking on a file and selecting New ➢ Compressed (Zipped) Folder. When you create a compressed folder, it will be displayed as a folder with a zipper.

Managing Data Encryption with EFS

Data encryption is a way to increase data security. Encryption is the process of translating data into code that is not easily accessible. Once data has been encrypted, you must have a password or key to decrypt the data. Unencrypted data is known as *plain text*, and encrypted data is known as *cipher text*.

The *Encrypting File System (EFS)* is the Windows Vista technology that is used to store encrypted files on NTFS partitions. Encrypted files add an extra layer of security to your file system. A user with the proper key can transparently access encrypted files. A user without the proper key is denied access. If the user who encrypted the files is unavailable, you can use the *data recovery agent (DRA)* to provide the proper key to decrypt folders or files.

In the following sections you will learn about the features for EFS in Windows Vista, how to create and manage DRAs, how to recover encrypted files, how to share encrypted files, and how to use the Cipher utility.

EFS Features in Windows Vista

The EFS features included with Windows Vista include the following:

- Automatically color-codes encrypted files in green text, so you can easily identify files that have been encrypted
- Support so that offline folders can also be encrypted
- A shell user interface (UI) that is used to support encrypted files for multiple users
- Control over who can read the encrypted files

Encrypting and Decrypting Folders and Files

To use EFS, a user specifies that a folder or file on an NTFS partition should be encrypted. The encryption is transparent to users. However, when other users try to access the file, they will not be able to unencrypt the file—even if those users have Full Control NTFS permissions. Instead, they will receive an error message.

To encrypt a folder or a file, take the following steps:

1. Select Start and type **Explorer** in the Search box.
2. In Windows Explorer, find and select the folder or file you wish to encrypt.
3. Right-click the folder or file and select Properties from the context menu.
4. On the General tab of the folder's or file's Properties dialog box, click the Advanced button.
5. The Advanced Attributes dialog box appears. Check the Encrypt Contents to Secure Data check box. Then click OK.
6. The Confirm Attribute Changes dialog box appears. Specify whether you want to apply encryption only to this folder (Apply Changes to This Folder Only) or to the subfolders and files in the folder as well (Apply Changes to This Folder, Subfolders and Files). Then click OK.

To decrypt folders and files, repeat these steps, but uncheck the Encrypt Contents to Secure Data option in the Advanced Attributes dialog box.

In Exercise 7.5, you will use EFS to encrypt a folder. This exercise assumes that you have completed Exercise 7.1.

EXERCISE 7.5

Using EFS to Manage Data Encryption

1. Use the Local Users and Groups utility to create the new user **Lauren**. (See Chapter 5 for details on creating user accounts.) Deselect the User Must Change Password at Next Logon option for this user.
2. Select Start and type **Explorer** in the Search box.
3. In Windows Explorer, find and select a folder on the D: drive. The folder you select should contain files. Right-click the folder and select Properties.
4. On the General tab of the folder's Properties dialog box, click the Advanced button.
5. In the Advanced Attributes dialog box, check the Encrypt Contents to Secure Data option. Then click OK.
6. In the Confirm Attribute Changes dialog box (if this dialog box does not appear, click the Apply button in the Properties dialog box to display it), select Apply Changes to This Folder, Subfolders and Files. Then click OK.

EXERCISE 7.5 *(continued)*

7. Log off as Administrator and log on as Lauren.
8. Open Windows Explorer and attempt to access one of the files in the folder you encrypted. You should receive an error message stating that the file is not accessible.
9. Log off as Lauren and log on as Administrator.

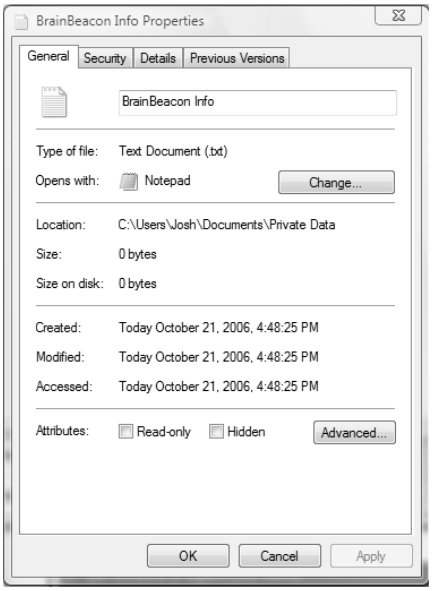
Managing EFS File Sharing

In Windows Vista, it is possible to share encrypted files with another person or between two computers. To share encrypted files, you must have a valid EFS certificate for the user who should have access to the file. By implementing EFS file sharing, you provide an additional level of recovery in the event that the person who encrypted the files is unavailable.

To implement EFS file sharing, take the following steps:

1. Encrypt the file if it is not already encrypted (see the previous section for instructions).
2. Through Windows Explorer, access the encrypted file's properties, as shown in Figure 7.19. At the bottom of the dialog box, click the Advanced button.
3. The Advanced Attributes dialog box will appear, as shown in Figure 7.20.

FIGURE 7.19 An encrypted file's Properties dialog box

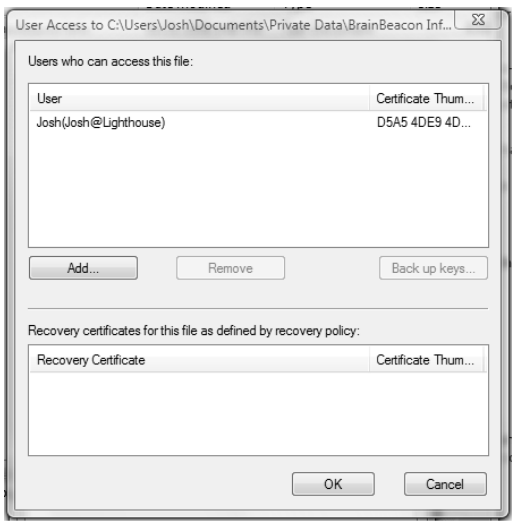


In the Compress or Encrypt Attributes section of the Advanced Attributes dialog box, click the Details button, which brings up the Encryption Details dialog box shown in Figure 7.21.

4. In the Encryption Details dialog box, click the Add button to add any additional users (provided they have a valid certificate for EFS in Active Directory or that you have imported a valid certificate onto the local computer) who should have access to the encrypted file.

FIGURE 7.20 Advanced Attributes dialog box

FIGURE 7.21 Encryption Details dialog box



Using the DRA to Recover Encrypted Files

If the user who encrypted the folders or files is unavailable to decrypt the folders or files when they're needed, you can use the data recovery agent (DRA) to access the encrypted files. DRAs are implemented differently depending on the version of your operating system and the configuration of your computer.

- For Windows Vista computers that are a part of a Windows 2003 Active Directory domain, the domain Administrator user account is automatically assigned the role of DRA.
- For Windows Vista computers that are installed as stand-alone computers or if the computer is a part of a workgroup, no default DRA is assigned.

You should use extreme caution when using EFS on a stand-alone Windows Vista computer. If the key used to encrypt the files is lost, there is no default recovery process, and all access to the files will be lost.

Creating a DRA on a Stand-Alone Windows Vista Computer

If Windows Vista is installed on a stand-alone computer or on a computer that is part of a workgroup, then no DRA is created by default. To manually create a DRA, you use the Cipher command-line utility as follows:

```
Cipher /R:filename
```

The `/R` switch is used to generate two files, one with a `.pfx` extension and one with a `.cer` extension. The `.pfx` file is used for data recovery and the `.cer` file includes a self-signed EFS recovery agent certificate. The `.cer` file (self-signed public key certificate) can then be imported into the local security policy and the `.pfx` file (private key) can be stored in a secure location.

Once you have created the public and private keys to be used with EFS, you can specify the DRA through Local Security Policy, using the following steps:

1. Through Local Security Policy, which can be accessed through Administrative Tools or the Local Computer Policy MMC snap-in, expand Public Key Policies and then Encrypting File System, as shown in Figure 7.22.
2. Right-click Encrypting File System and select Add Data Recovery Agent.
3. The Add Recovery Agent Wizard will start. Click the Next button to continue.
4. The Select Recovery Agents screen will appear, as shown in Figure 7.23. Click the Browse Folders button to access the `.cer` file you created with the `Cipher /R:filename` command. Select the certificate and click Next.
5. The Completing the Add Recovery Agent Wizard screen will appear. Confirm that the settings are correct and click the Finish button.

You will see the Data Recovery Agent listed in the Local Security Settings dialog box, under Encrypting File System.

FIGURE 7.22 Local Security Settings dialog box

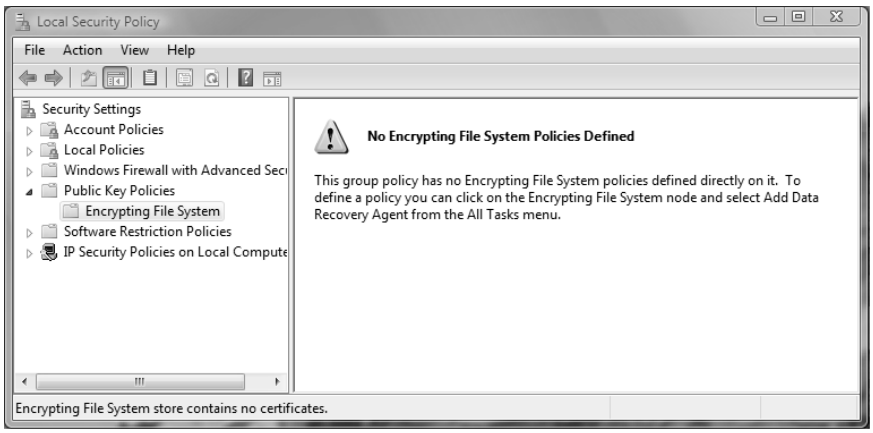
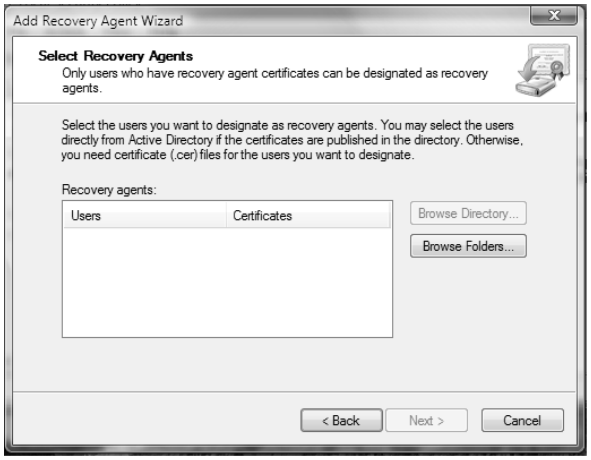


FIGURE 7.23 Select Recovery Agents screen of the Add Recovery Agent Wizard



Recovering Encrypted Files

If the DRA has the private key to the DRA certificate (that was created through `Cipher /R:`*`filename`*), the DRA can decrypt files in the same manner as the user who originally encrypted the file. Once the encrypted files are opened by a DRA, they are available as unencrypted files and can be stored as either encrypted or unencrypted files.

Using the Cipher Utility

Cipher is a command-line utility that can be used to encrypt files on NTFS volumes. The syntax for the `Cipher` command is as follows:

`Cipher /[command parameter] [filename]`

Table 7.2 lists common command parameters associated with the `Cipher` command.

TABLE 7.2 Cipher Command Parameters

Parameter	Description
`/E`	Specifies that files or folders should be encrypted. Any files that are subsequently added to the folder will be encrypted.
`/D`	Specifies that files or folders should be decrypted. Any files that are subsequently added to the folder will not be encrypted.
`/S:dir`	Specifies that subfolders of the target folder should also be encrypted or decrypted based on the option specified.
`/I`	Causes any errors that occur to be ignored. By default, the Cipher utility stops whenever an error occurs.
`/H`	By default, files with hidden or system attributes are omitted from display. This option specifies that hidden and system files should be displayed.
`/K`	Creates a new certificate file and certificate key.
`/R`	Used to generate a recovery agent key and certificate for use with EFS.
`/X`	Used to back up the EFS certificate and keys into the specified file name.

In Exercise 7.6, you will use the Cipher utility to encrypt files. This exercise assumes that you have completed Exercise 7.5.

EXERCISE 7.6

Using the Cipher Utility

1. Select Start ➢ All Programs ➢ Accessories ➢ Command Prompt.
2. In the Command Prompt dialog box, type **D:** and press Enter to access the D: drive.
3. From the `D:\>` prompt, type **cipher**. You will see a list of folders and files and the state of encryption. The folder you encrypted in Exercise 7.5 should be indicated by an *E*.

EXERCISE 7.6 *(continued)*

4. Type **MD TEST** and press Enter to create a new folder named `Test`.
5. Type **`cipher /e test`** and press Enter. You will see a message verifying that the folder was encrypted.

Using the Disk Defragmenter Utility

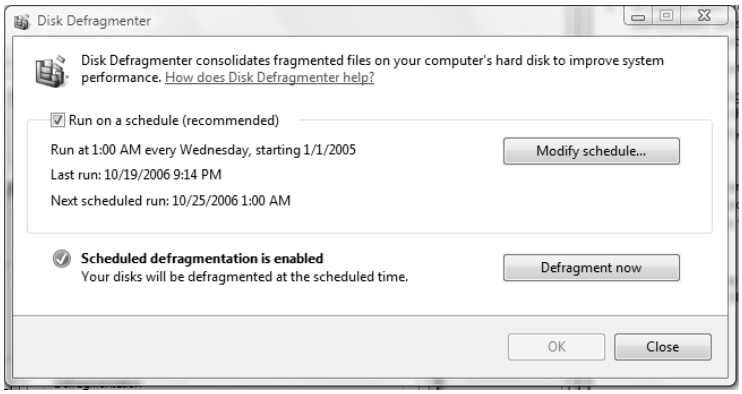
Data is normally stored sequentially on the disk as space is available. *Fragmentation* naturally occurs as users create, delete, and modify files. The access of noncontiguous data is transparent to the user; however, when data is stored in this manner, the operating system must search through the disk to access all the pieces of a file. This slows down data access.

Disk defragmentation rearranges the existing files so they are stored contiguously, which optimizes access to those files. In Windows Vista, you use the *Disk Defragmenter utility* to defragment your disk.

To access the Disk Defragmenter, select Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools ➢ Computer Management; expand Storage and select Disk Management; right-click the drive to defragment; select the Tools tab; and then click the Defragment Now button. The Disk Defragmenter window is displayed, as shown in Figure 7.24; you can schedule when the Disk Defragmenter should run or run the Disk Defragmenter tool immediately.

You can also defragment disks through the command-line utility, Defrag. The disk needs to have at least 15 percent free space for Defrag to run properly. You can analyze the state of the disk by using `Defrag` *`VolumeName`* `/a`.

FIGURE 7.24 The Disk Defragmenter window



Using the Disk Cleanup Utility

The *Disk Cleanup utility* identifies areas of disk space that can be deleted to free hard disk space. Disk Cleanup works by identifying temporary files, Internet cache files, and unnecessary program files.

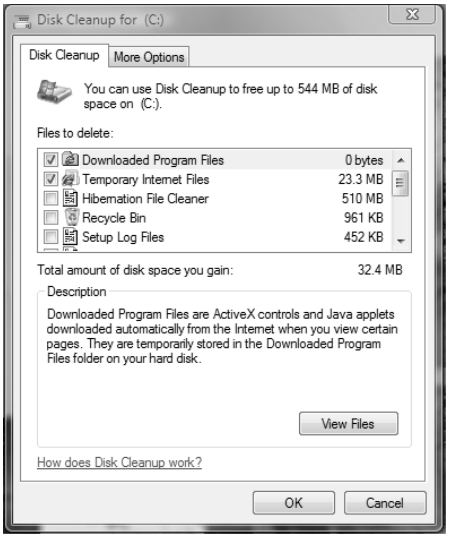
To access this utility, select Start ➢ Control Panel ➢ System and Maintenance ➢ Free Up Disk Space. You select the drive you want to clean up, and the Disk Cleanup utility then runs and calculates the amount of disk space you can free up.

In Exercise 7.7, you will use the Disk Cleanup utility.

EXERCISE 7.7

Using the Disk Cleanup Utility

1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Free Up Disk Space.
2. In the Disk Cleanup Options dialog box, select the Files from All Users on This Computer option.
3. Select the C: drive, and click OK.



4. After the analysis is complete, you will see the Disk Cleanup dialog box, listing files that are suggested for deletion and showing how much space will be gained by deleting those files. For this exercise, leave all the boxes checked and click OK.
5. When you are asked to confirm that you want to delete the files, click the Yes button. The Disk Cleanup utility deletes the files and automatically closes the Disk Cleanup dialog box.

Troubleshooting Disk Devices and Volumes

If you are having trouble with your disk devices or volumes, you can use the Windows Vista *Check Disk utility*. This utility detects bad sectors, attempts to fix errors in the file system, and scans for and attempts to recover bad sectors. In order to use Check Disk you must be logged in as a member of the Administrators group.

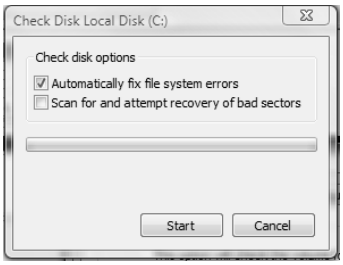
File system errors can be caused by a corrupted file system or by hardware errors. If you have software errors, the Check Disk utility may help you find them. There is no way to fix hardware errors through software, however. If you have excessive hardware errors, you should replace your disk drive.

In Exercise 7.8, you will run the Check Disk utility.

EXERCISE 7.8

Using the Check Disk Utility

1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools.
2. Double-click Computer Management, and then expand Storage and select Disk Management.
3. Right-click the D: drive and choose Properties.
4. Click the Tools tab, and then click the Check Now button.
5. In the Check Disk dialog box, you can choose one or both of the options to automatically fix file system errors and to scan for and attempt recovery of bad sectors. For this exercise, check both of the disk options check boxes. Then click the Start button.



The Check Disk utility can also be run from the command line, using the command Chkdsk. Chkdsk is used to create and display a status report, which is based on the file system you are using.

Summary

In this chapter, you learned about disk management with Windows Vista. We covered the following topics:

- File system configuration, which can be FAT32 or NTFS. You also learned how to convert a FAT32 partition to NTFS by using the Convert command-line utility.
- Disk storage configuration, which can be basic storage or dynamic storage. Dynamic storage is used to create simple volumes, spanned volumes, and striped volumes.
- The Disk Management utility, which you use to manage routine tasks, basic storage, and dynamic storage.
- Data compression, which is used to store files in a compressed format that uses less disk space.
- Data encryption, which is implemented through the Encrypting File System (EFS) and provides increased security for files and folders.
- Disk defragmentation, which is accomplished through the Disk Defragmenter utility and allows you to store files contiguously on your hard drive for improved access speeds.
- The Disk Cleanup utility, which is used to free disk space by removing unnecessary files.
- The Check Disk utility, which can be used to troubleshoot disk errors.
- Troubleshooting disks and volumes, which is used in the event of disk or volume errors or for maintenance.

Exam Essentials

Be able to configure and manage file systems. Understand the differences and features of the FAT32 and NTFS file systems. Know how to configure options that are specific to the NTFS file system. Understand that you can convert a file system from FAT32 to NTFS but that you can't convert from NTFS to anything else.

Know how to monitor and configure disks. Use the Disk Management utility to configure disks for simple, spanned, or striped volumes. Be aware of the lack of fault tolerance in disk configurations used by Windows Vista. Be able to use Disk Management to monitor disks for physical drive and logical drive errors. Be familiar with both the Disk Cleanup utility and the Disk Defragmenter utility.

Know how to use disk compression. Understand what types of files can benefit from disk compression and be able to configure and manage compressed folders and files.

Be able to use encryption to protect files. Know when it is appropriate to use encryption. Know how to manage encryption through Windows Explorer, as well as through the Cipher command-line utility. Know how to recover encrypted files if the user who encrypted the files is unavailable.

Be able to troubleshoot disks and volumes. Know what options and utilities can be used to troubleshoot disks and volumes and be able to repair disks and volumes that are not functioning properly.

Review Questions

1. Steve has installed Windows Vista on his computer. He has FAT32 and NTFS partitions. In addition, he boots his computer to Windows XP Professional for testing an application he is writing, checking for compatibility with both operating systems. Which of the following file systems will be seen by both operating systems?
   - **A.** Only the FAT32 partition will be seen by both operating systems.
   - **B.** Only the NTFS partition will be seen by both operating systems.
   - **C.** Neither the FAT32 partition nor the NTFS partition will be seen by both operating systems.
   - **D.** Both the FAT32 partition and the NTFS partition will be seen by both operating systems.

2. Jack has an NTFS partition on his Windows Vista computer. He wants to dual-boot to a Linux distribution to perform testing on a cross-platform application his company created. What command or utility should he use to convert his NTFS partition to FAT32?
   - **A.** Convert.
   - **B.** Disk Administrator.
   - **C.** Disk Manager.
   - **D.** This operation is not supported.

3. Brad is the payroll manager and stores critical files on his local drive for added security on his Windows Vista computer. He wants to ensure that he is using the disk configuration with the most fault tolerance and the highest level of consistent availability. Which of the following provisions should he use?
   - **A.** Disk striping
   - **B.** Spanned volumes
   - **C.** Mirrored volumes
   - **D.** A good backup scheme

4. Carrie is considering upgrading her basic disk to a dynamic disk on her Windows Vista computer. She asks you for help in understanding the function of dynamic disks. Which of the following statements are true of dynamic disks in Windows Vista? (Choose all that apply.)
   - **A.** Dynamic disks can be recognized by older operating systems such as Windows NT 4, in addition to new operating systems such as Windows Vista.
   - **B.** Dynamic disks are supported only by Windows 2000 Server and Windows Server 2003.
   - **C.** Dynamic disks support features such as simple volumes, extended volumes, spanned volumes, and striped volumes.
   - **D.** Dynamic disks support features such as simple volumes, extended volumes, spanned volumes, mirrored volumes, and striped volumes.

5. Linda is using Windows Vista on her laptop computer, and the C: partition is running out of space. You want to identify any areas of free space that can be reclaimed from temporary files. What utility should you use?

   A. Disk Cleanup

   B. Disk Manager

   C. Disk Administrator

   D. Disk Defragmenter

6. Greg is using Windows Vista to store video files. He doesn't access the files very often and wants to compress the files to utilize disk space. Which of the following options allows you to compress files in Windows Vista?

   A. `Compress.exe`

   B. `Cipher.exe`

   C. `Packer.exe`

   D. Windows Explorer

7. Susan wants the highest level of security possible for her data. She stores the data on an NTFS partition and has applied NTFS permissions. Now she wants to encrypt the files through EFS (Encrypting File System). Which command-line utility can she use to manage data encryption?

   A. Encrypt

   B. Cipher

   C. Crypto

   D. EFS

8. You have compressed a 4MB file into 2MB. You are copying the file to another computer that has a FAT32 partition. How can you ensure that the file will remain compressed?

   A. When you copy the file, use the `XCOPY` command with the `/Comp` switch.

   B. When you copy the file, use the Windows Explorer utility and specify the option Keep Existing Attributes.

   C. On the destination folder, make sure that you set the option Compress Contents to Save Disk Space in the folder's properties.

   D. You can't maintain disk compression on a non-NTFS partition.

9. Julie wants to allow her assistant, Sam, access to several files that she has encrypted with EFS. How can she allow Sam to access the files on Julie's computer?

   A. Julie should export and e-mail Sam her encryption key.

   B. Julie should configure NTFS permissions to provide Sam full access to the files.

   C. Julie should configure share permissions to provide Sam with full access to the files over the network.

   D. Julie should import Sam's encryption key and add Sam's certificate to each file Sam should have access to.

10. Tom is the manager of Human Resources in your company. He is concerned that members of the Administrators group, who have implied access to all NTFS resources, will be able to easily view the contents of the sensitive personnel files. What is the highest level of security that can be applied to the payroll files?

    A. Apply NTFS permissions to the files.

    B. Encrypt the files with EFS.

    C. Secure the files with the `Secure.exe` command.

    D. Encrypt the files with HSP.

11. Scott frequently works with a large number of files. He is noticing that the larger the files get, the longer it takes to access them. He suspects that the problem is related to the files being spread over the disk. What utility can be used to store the files sequentially on the disk?

    A. Disk Cleanup

    B. Disk Manager

    C. Disk Administrator

    D. Disk Defragmenter

12. You are the network administrator for a small company. You have a laptop that you use to test an application that is deployed to several users who only have access to a Windows 98 computer. To accommodate the testing of the application, you have a laptop that dual-boots between Windows Vista and Windows 98. You currently have Windows Vista on drive C: and Windows 98 on drive D:. Both partitions are formatted with FAT32. You decide to convert the C: drive to NTFS so that you can apply additional security to some of the files. You use the Convert command-line utility to convert the D: drive. Before you reboot and convert the drive, you realize that data on the drive needs to be accessed from the Windows 98 operating system. How can you cancel the conversion process?

    A. Use `Convert D: /cancel`.

    B. Use `Convert D: /fs:FAT`.

    C. In Disk Administrator, select Tools ➢ Cancel Conversion for Drive C:.

    D. Edit the Registry setting for `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager` to `autocheck autochk *`.

13. Cindy is the payroll manager at your company. The day before the payroll is processed, Cindy is involved in a minor car accident and spends two days in the hospital. She has Windows Vista installed as a part of a workgroup and has encrypted the payroll files with EFS. All of the EFS settings for the computer are set to default values. How can these files be accessed in her absence?

    A. The Administrator user account can access the files by backing up the files, restoring the files on the computer where the recovery agent is located, and disabling the files' Encrypt the Contents to Secure Data option.

    B. The Administrator user account can access the files by using the `unencrypt` command-line utility.

    C. The Administrator user account can access the files by using the `encrypt -d` command.

    D. Unless a DRA has been configured, there will be no access to the files.

14. You have an extremely large database that needs to be stored on a single partition. Your boss asks you about the maximum capacity for an NTFS partition, assuming you are using 4KB clusters. What is the correct answer?

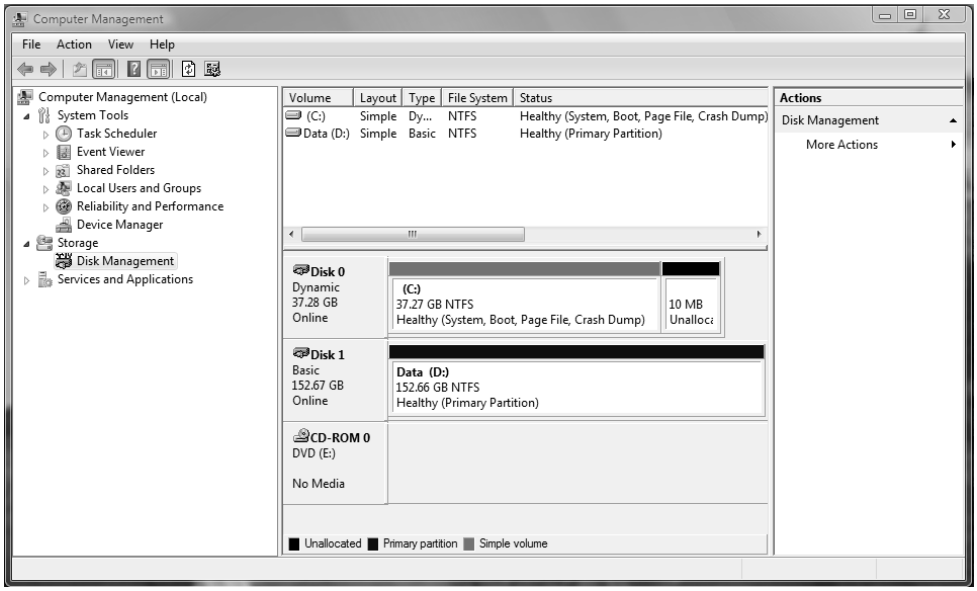
A. 32GB

B. 64GB

C. 132GB

D. 16TB

15. You have just added a new disk to your computer that supports hot swapping. Your computer now has three physical drives. When you look at Disk Management, you see the screen shown here. What is the fastest way to allow Windows Vista to recognize the new disk?



A. Restart the computer.

B. In Disk Manager, select Action ➢ Rescan Disk.

C. In Disk Management, select Action ➢ Rescan Disk.

D. In System Tools, select Update Disks.

16. You have an 8MB image file that you want to e-mail to another user in the marketing department. Which of the following should you do in order to e-mail the image?

A. Encrypt the image with EFS.

B. Configure compression on the directory in which the image file is stored.

C. Right-click the image file and select Send To ➢ Compressed (Zipped) folder.

D. Use the Compact command-line utility.

17. You are installing a new hard drive into your computer, which dual-boots between Windows Vista and Windows XP. You will be storing large and sensitive files on this drive. You will need to access these files from either operating system. You need to determine the file system to use when formatting the disk. Which of the following should you use?

    A. NTFS

    B. FAT32

    C. FAT16

    D. CDFS

18. You are administering a Windows Vista computer. You suspect that the disk in the computer may have some bad sectors. You want to determine if the disk does have any bad sectors and fix them if possible. Which utility could you use to accomplish this?

    A. DiskPart

    B. Check Disk

    C. Disk Cleanup

    D. Disk Defragmenter

19. You are the human resources administrator for your company. You have recently been assigned a Windows Vista laptop computer. You have added a new directory named HR to the computer. You want to ensure that all files that are stored within the HR directory are encrypted. You will use the Cipher utility to accomplish this. Which of the following options should you use with the Cipher utility?

    A. `/D`

    B. `/E`

    C. `/R`

    D. `/X`

20. You are a system administrator for your company. You are managing a Windows Vista computer. You issue the following command at a command prompt:`Compact /C`. Which of the following will occur as a result of issuing this command?

    A. All files located on the C: drive will be compressed.

    B. All files located on the C: drive will be uncompressed.

    C. All files within the specified directory will be compressed.

    D. All files within the specified directory will be uncompressed.

Answers to Review Questions

1. D. Both Windows Vista and Windows XP Professional support FAT32 and the NTFS file systems, so both file systems will be viewable on both operating systems.

2. D. You can convert from FAT32 to NTFS, but it is a one-way process if you want to preserve your data. You cannot convert from NTFS back to FAT32 without first deleting all existing partitions.

3. D. Windows Vista supports simple, spanned, and striped volumes. Mirrored volumes are available with Windows 2000 Server and Windows Server 2003. Brad should make sure he has a good backup for reliability.

4. C. Dynamic disks are supported by Windows Vista, as well as by Windows XP, Windows 2000, and Windows Server 2003. There is no support for mirrored volumes in Windows Vista. Windows 2000 Server and Windows Server 2003 supports mirrored volumes and RAID-5 configurations.

5. A. The Disk Cleanup utility is used to identify areas of space that may be reclaimed through the deletion of temporary files or Recycle Bin files. You access this utility through Start ➢ Control Panel, click System and Maintenance, then click Free Up Disk Space, which is located under Administrative Tools in the System and Maintenance window.

6. D. In Windows Vista, one way you can compress files is through Windows Explorer. Windows Vista has no programs called `COMPRESS` or `PACKER`. The Cipher program is used to encrypt or decrypt files. The command-line options for managing file and folder compression are `COMPACT` and `EXPAND`.

7. B. The Cipher utility is used to encrypt or decrypt files. Windows Vista doesn't have a program called Encrypt, Crypto, or EFS. If you want to manage file encryption through a GUI utility, you can use Windows Explorer.

8. D. Windows Vista data compression is supported only on NTFS partitions. If you move the file to a FAT32 partition, then it will be stored as uncompressed.

9. D. To allow Sam to access Julie's encrypted files, Julie should import Sam's encryption key and then add that key to each file to which Sam should have access. Adding share permissions or NTFS permissions will not allow another user to access an encrypted file unless that user's encryption key has been added to the file. Exporting and e-mailing Julie's key to Sam will not allow Sam to access the file.

10. B. You can increase the level of security on folders and files on an NTFS partition by using Encrypting File System (EFS). Only a user who is configured as a DRA with the correct private key or who has explicitly been provided permission can access this data.

11. D. The Disk Defragmenter utility is used to rearrange files so that they are stored contiguously on the disk. This optimizes access to those files. You can also defragment disks through the command-line utility, Defrag.

12. D. The only way to cancel an NTFS conversion prior to reboot is to edit the Registry setting for `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager` to `autocheck autochk *`. Once the conversion has taken place, there is no way to reverse the conversion process.

13. D. By default, a Windows Vista computer that is installed as a stand-alone computer or a part of a workgroup has no DRA automatically configured. You will not be able to access her files.

14. D. You can have NTFS partitions that are up to 16TB with 4KB clusters or 256TB with 64KB clusters. NTFS supports the largest partitions of any of the file systems supported by Windows Vista.

15. C. Select Action ➢ Rescan Disk in the Disk Management utility. The disk will then be listed through the Disk Management utility and can be configured as needed.

16. C. You can send the image in a compressed file in order to limit the size of the image while e-mailing it. Compressing an image in a zipped file can often drastically reduce the size of the image file and make it easier to e-mail to other users. To send the image file to a compressed folder, you can right-click the file and select Send To ➢ Compressed (Zipped) Folder.

17. A. You should use NTFS when formatting the new disk. Only NTFS supports both file encryption and file compression. Both Windows XP and Windows Vista can access NTFS partitions, so file access should not be a problem.

18. B. To check a disk to determine if it has any bad sectors, you can use the Check Disk utility, which can be access from the command line by typing `Chkdsk`. The Check Disk utility can discover and attempt to fix bad sections on hard disks.

19. B. You should use the `/E` option with the Cipher utility. The `/E` option encrypts the specified directory and configures all files subsequently added to the directory to be encrypted.

20. C. By issuing the command `Compact /C`, you ensure that all files within the specified directory will be compressed. The Compact utility can be used to compress files and directories from a command line. The `/C` option compresses the selected files.

Chapter

8

Configuring Network Connectivity

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring Network Connectivity**
  - Configure networking by using the Network and Sharing Center
  - Configure Remote Access
  - Troubleshoot connectivity issues

For successful network connection management, you must have a properly installed and configured network adapter and network protocol. The first step is physically installing and configuring the network adapter you will use. The second step is installing and configuring the network protocol used by your network.

In this chapter, you will first learn how to install and configure network adapters. Next, you will learn about the Network and Sharing Center, remote access, network projectors, and printers. You will also learn about how wireless network adapters work and how to configure security for small wireless networks. Finally, you will learn about network connectivity troubleshooting.

Installing and Configuring Network Adapters

Network adapters are hardware used to connect computers (or other devices) to the network. Network adapters are responsible for providing the physical connection to the network and the physical address of the computer. These adapters (and all other hardware devices) need a *driver* to communicate with the Windows Vista operating system.

In the following sections, you will learn how to install and configure network adapters, as well as how to configure authentication, including advanced settings, and how to manage network bindings for your adapters. Finally, you will learn how to troubleshoot network adapters that are not working.

Installing a Network Adapter

Before you physically install your network adapter, it's important to read the instructions that came with the hardware. If your network adapter is new, it should be self-configuring, with Plug and Play capabilities. After you install a network adapter that supports Plug and Play, it should work the next time you start up the computer.

New devices will autodetect settings and be self-configuring. Older devices rely on hardware setup programs to configure hardware. Really old devices require you to manually configure the adapter through switches or jumpers.

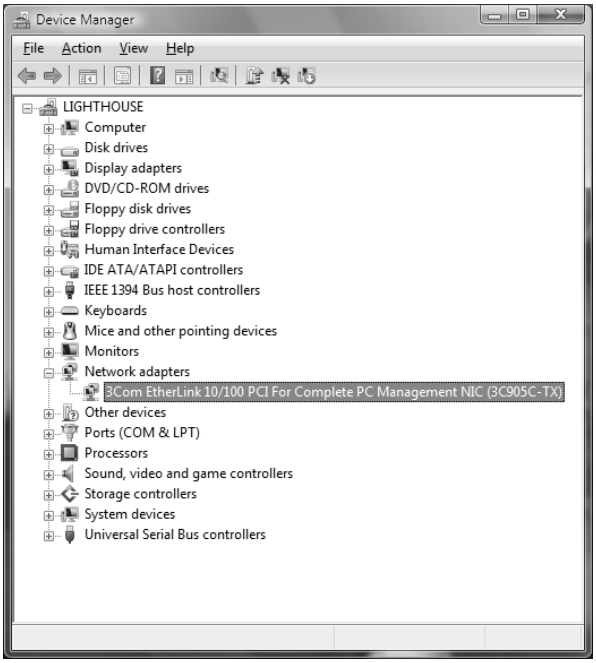
When you install a network adapter that is not Plug and Play, the operating system should detect that you have a new piece of hardware and start a wizard that leads you through the process of loading the adapter's driver.

Configuring a Network Adapter

Once the network adapter has been installed, you can configure it through its Properties dialog box. To access this dialog box, select Start ➢ Computer ➢ System Properties➢ Device Manager. From Device Manager, expand the Network Adapters icon and double-click the network device, as shown in Figure 8.1.

You can also access the network adapter's Properties dialog box by selecting Start ➢ Network ➢ Network and Sharing Center ➢ Manage Network Connections, right-clicking the Local Area Connection icon, selecting Properties, and clicking the Configure button. However, by doing so, you will not have access to the Resources tab, which is discussed in detail later in this chapter.

FIGURE 8.1 Device Manager showing the network adapter

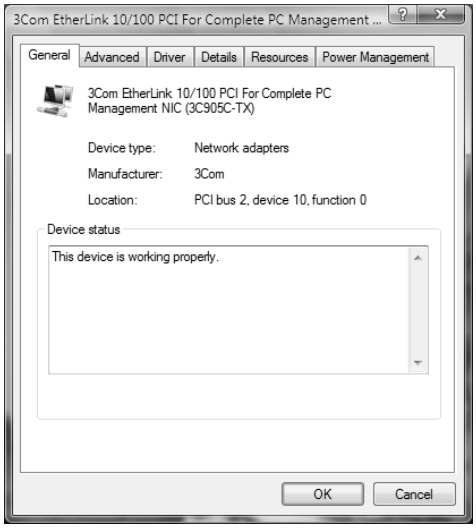


In the network adapter Properties dialog box, the properties are grouped on six tabs: General, Advanced, Driver, Details, Resources, and Power Management. We explain these properties in the following sections.

General Network Adapter Properties

The General tab of the network adapter Properties dialog box, shown in Figure 8.2, shows the name of the adapter, the device type, the manufacturer, and the location. The Device Status box reports whether the device is working properly.

FIGURE 8.2 The General tab of the network adapter's Properties dialog box

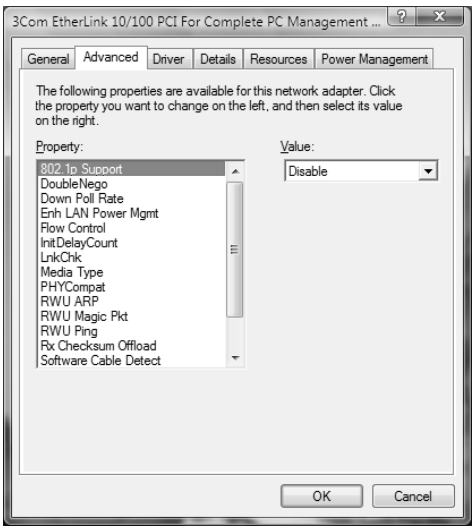


Advanced Network Adapter Properties

The contents of the Advanced tab of a network adapter's Properties dialog box vary depending on the network adapter and driver that you are using. Figure 8.3 shows an example of the Advanced tab for a Fast Ethernet adapter. To configure options in this dialog box, choose the property you want to modify in the Property list box on the left and specify the value for the property in the Value box on the right.

You should not need to change the settings on the Advanced tab of the network adapter's Properties dialog box unless you have been instructed to do so by the manufacturer.

FIGURE 8.3 The Advanced tab of the network adapter's Properties dialog box



Driver Properties

The Driver tab of the network adapter Properties dialog box, shown in Figure 8.4, provides the following information about your driver:

- The driver provider, which is usually Microsoft or the network adapter manufacturer
- The date that the driver was released
- The driver version, which is useful in determining whether you have the latest driver installed
- The digital signer, which is the company that provides the digital signature for driver signing

Clicking the Driver Details button on the Driver tab brings up the Driver File Details dialog box, as shown in Figure 8.5. This dialog box lists the following details about the driver:

- The location of the driver file, which is useful for troubleshooting
- The original provider of the driver, which is usually the manufacturer
- The file version, which is useful for troubleshooting
- Copyright information about the driver
- The digital signer for the driver

To update a driver, click the Update Driver button on the Driver tab. This starts a wizard that will step you through upgrading the driver for an existing device.

FIGURE 8.4 The Driver tab of the network adapter Properties dialog box

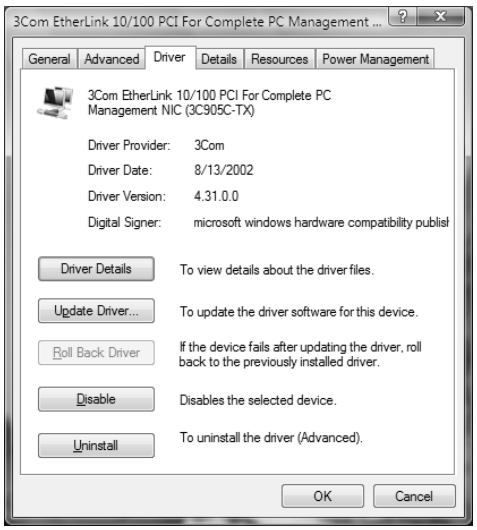
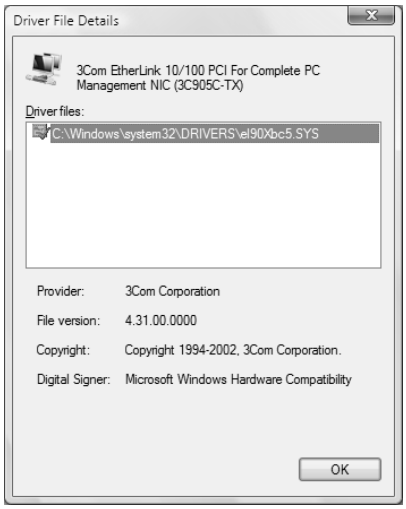


FIGURE 8.5 The Driver File Details dialog box



The Roll Back Driver feature is activated by clicking the Roll Back Driver button. This button allows you to roll back to the previously installed driver if you update your network driver and encounter problems.

The Disable button is used to disable the device. After you disable the device, the Disable button changes into an Enable button, which can be used to enable the device.

The Uninstall button at the bottom of the Driver tab removes the driver from your computer. You would uninstall the driver if you were going to remove the device from your system or if you want to completely remove the driver from your system so that you can reinstall it from scratch. Normally, you would want to update the driver rather than uninstall it and reinstall it.

If you cannot find the driver or the configuration instructions for your network card, check the vendor's website. Usually, you will be able to find the latest drivers. You also should be able to locate a list of Frequently Asked Questions (FAQs) about your hardware.

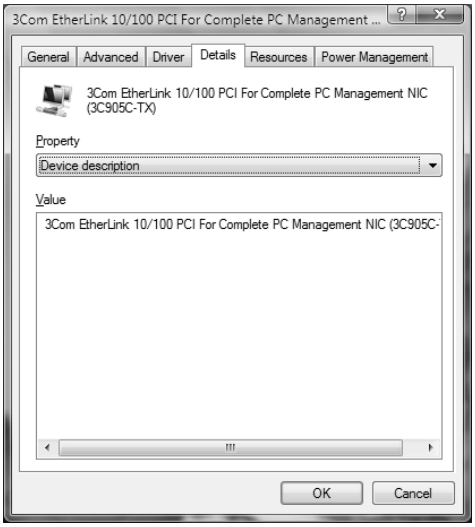
Details Properties

The Details tab of the network adapter's Properties dialog box is new to Windows Vista. This tab lists the resource settings for your network adapter, as shown in Figure 8.6. Information found on the Details tab can include the device description, bus number, address, problem code, INF name, and driver information.

Resource Properties

Each device installed on a computer uses computer resources. Resources include interrupt request (IRQ), memory, and I/O (input/output) resources. The Resources tab of the network adapter's Properties dialog box lists the resource settings for your network adapter, as shown in Figure 8.7. This information is important for troubleshooting, because if other devices are trying to use the same resource settings, your devices will not work properly. The Conflicting Device List box at the bottom of the Resources tab shows whether there are any conflicts with other devices.

FIGURE 8.6 The Details tab of the network adapter's Properties dialog box



Power Management Properties

The Power Management tab of the network adapter's Properties dialog box lists the power management settings for your network adapter, as shown in Figure 8.8. On this tab, you can allow the computer to turn off the network card to save power. You can also configure the network card to be able to wake the computer from standby mode, and whether you want only management stations to be able to wake the computer.

FIGURE 8.7 The Resources tab of the network adapter's Properties dialog box

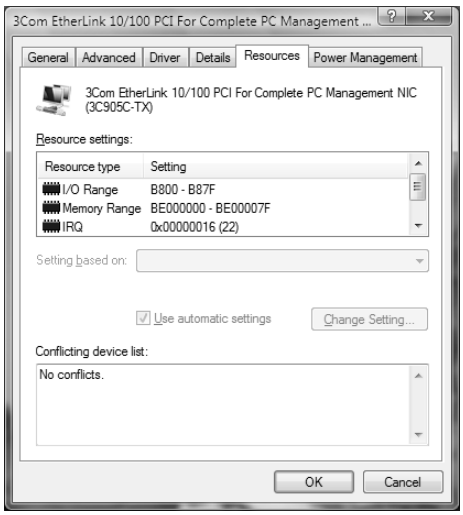
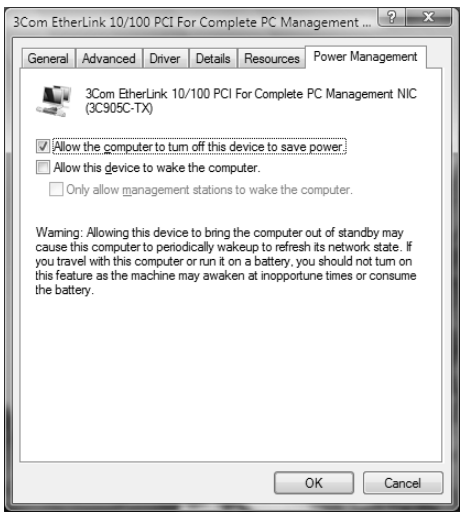


FIGURE 8.8 The Power Management tab of the network adapter's Properties dialog box



In Exercise 8.1, you will view the properties of your network adapter. This exercise assumes you have a network adapter installed in your computer.

EXERCISE 8.1

Viewing Network Adapter Properties

1. Select Start ➢ Network ➢ Network and Sharing Center. In the Network and Sharing Center dialog box, click the Manage Network Connections option.
2. You will see your Local Area Connection as an icon. Right-click Local Area Connection and select Properties. Click the Configure button.
3. On the General tab of the network adapter's Properties dialog box, verify that the Device Status box shows This Device Is Working Properly.
4. Click the Advanced tab. Note the properties that are available for your driver.
5. Click the Driver tab. Notice the driver date and version information. Click the Driver Details button to see the location of your network adapter's driver file. Click OK to close the Driver File Details dialog box.
6. Click the Details tab. Note the settings that are being used by your network adapter.
7. Click the Power Management tab. Note the power settings that are configured for your network card. Click OK to close the dialog box.

Troubleshooting Network Adapters

If your network adapter is not working, the problem may be with the hardware, the driver software, or the network protocols. The following are some common causes for network adapter problems:

Network adapter not on the HCL If the device is not on the HCL, contact the adapter vendor for advice.

Outdated driver Make sure that you have the most up-to-date driver for your adapter. You can check for the latest driver on your hardware vendor's website.

Network adapter not recognized by Windows Vista Check Device Manager to see if Windows Vista recognizes your device. If you do not see your adapter, you will have to manually install it (see "Installing a Network Adapter" earlier in this chapter).

Hardware that is not working properly Verify that your hardware is working properly. Run any diagnostics that came with the adapter. You can also select Diagnose from the Network Connections dialog box. If everything seems to work as it should, make sure that the cable is good and that all of the applicable network hardware is installed correctly and is working.

This is where it pays off to have spare hardware items (such as cables and extra network adapters) that you know work properly.

Improperly configured network protocols Make sure that your network protocols have been configured properly. Network protocols are covered in detail in the next section of this chapter.

Improperly configured network card Verify that all settings for the network card are correct.

Bad cable Make sure that all network cables are good. This can be tricky if you connect to the network through a patch panel.

Bad network connection device Verify that all network connectivity hardware is properly working. For example, on an Ethernet network, make sure the hub or switch and port that you are using are functioning properly.

Check Event Viewer for any messages that give you a hint about what is causing a network adapter error. See Chapter 11, "Maintaining and Optimizing Windows Vista," for details on using Event Viewer.

Real World Scenario

Are Ethernet Cards Properly Configured?

When you purchase Ethernet cards, they are usually special combo cards that support 10Mbps Ethernet and 100Mbps Fast Ethernet. Some even support 1000Mbps (or 1Gbps) Gigabit Ethernet. In addition, the cards have an RJ-45 connector for using unshielded twisted pair (UTP) cables. Older cards have a BNC connector for using coaxial cable.

A common problem is experienced with combo Ethernet cards. Even when the hardware configuration for IRQ and base memory is correctly configured and you have the right driver, the correct configuration for speed and cable type may not be detected. Within an Ethernet network, your Ethernet card must transmit at the same speed as the device to which it is connected. The card must also be configured to support the cable type being used. You can sometimes verify these settings through the network adapter's Properties dialog box. You can check the activity and speed of the connection in the Local Area Connection Status dialog box.

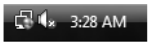
If the configuration is correct and you still can't connect to the network, you should check your network cables. It is estimated that between 70 and 80 percent of all network problems are related to cabling.

Using the Network and Sharing Center

The Network and Sharing Center is the new networking hub in Windows Vista. You can use the Network and Sharing Center to view and configure your network devices, as well as share files and printers on your network. You can get to the Network and Sharing Center in one of several ways:

- Click Start ➢ Network ➢ Network and Sharing Center.
- Click Start ➢ Control Panel ➢ Network and Internet ➢ Network and Sharing Center.
- Click Start ➢ Control Panel ➢ View Network Status and Tasks.
- Click Start ➢ Control Panel ➢ Classic View ➢ Network and Sharing Center.
- Click or right-click the Network icon (shown in Figure 8.9) on the right side of the taskbar, and click Network and Sharing Center.

FIGURE 8.9 Network icon indicating Internet access



If you have a network card installed, the networking icon should always be visible in the lower-right corner of the taskbar. If the Network icon is displayed with a globe, as it is in Figure 8.9, then your computer is connected to a network that has Internet access. If the Network icon is displayed without a globe, then your computer is connected to a network that is not connected to the Internet. Finally, if the Network icon is displayed with a red *X*, then the network adapter does not have any network connectivity.

The Network and Sharing Center dialog box, shown in Figure 8.10, contains four main areas:

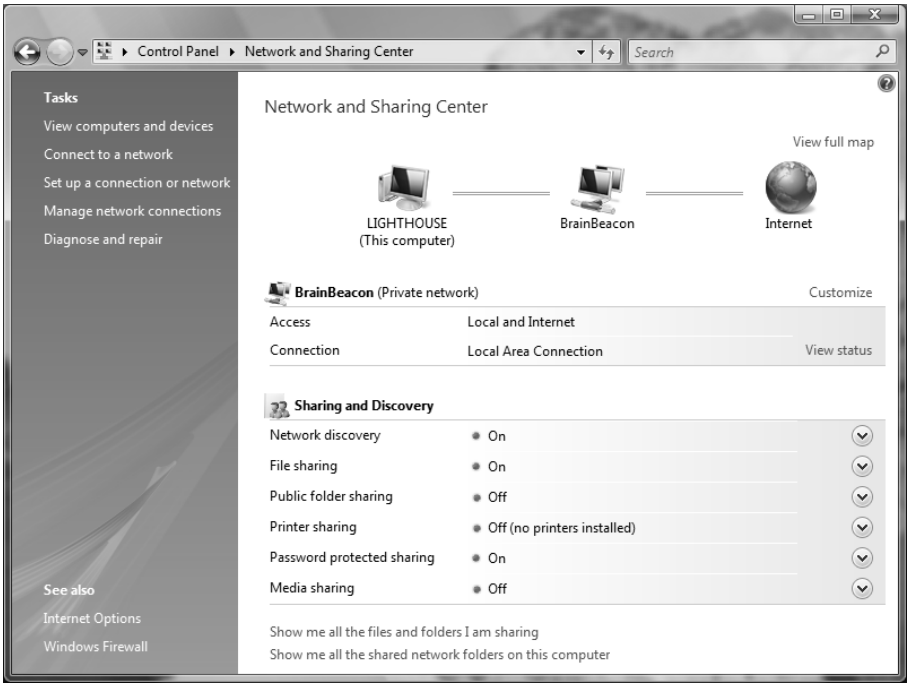
- Graphical view of your current connection
- Network information
- Sharing and Discovery
- Tasks

Graphical View

The graphical view displays your computer, the network to which you are connected, and the status of your connection to the Internet. If you want to view a full graphical map of all of the computers and devices to which you can connect, click View Full Map. The graphical map, shown in Figure 8.11, will show all of the devices on your network. The following list indicates computers and devices that might not be displayed within the network map:

- Windows Vista computers with network discovery turned off
- Windows Vista computers that are configured with the Public network setting

FIGURE 8.10 Network and Sharing Center



- Windows Vista computers with the Link Layer Topology Discovery (LLTD) protocol disabled
- Windows XP computers that do not have the LLTD protocol installed
- Computers that are preventing detection because of firewall settings
- Devices that do not support Universal Plug and Play (UPnP) or Web Services for Devices for Windows

Network Information

The Network information section contains the name of your network and the type of connection. The Customize link to the right of the network name brings up the Set Network Location dialog box, shown in Figure 8.12. This dialog box enables you to change the network name, change the network icon, and configure the network location to be Public or Private. You can also merge or delete network locations.

We will discuss Public and Private network locations in the following section.

FIGURE 8.11 Graphical view

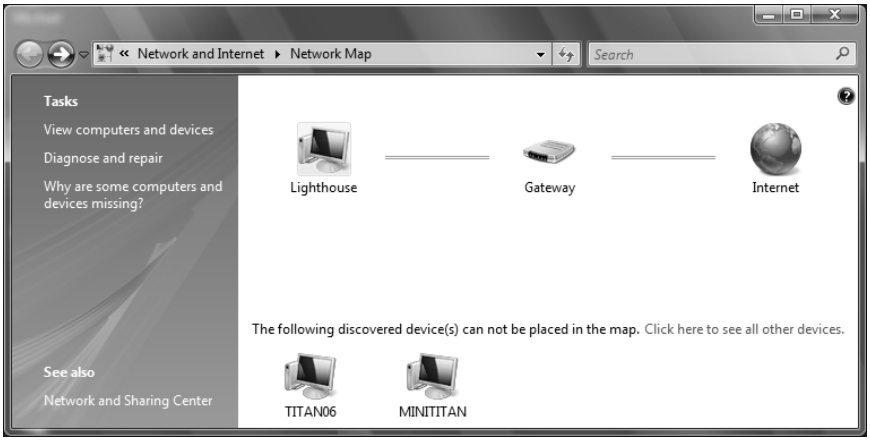
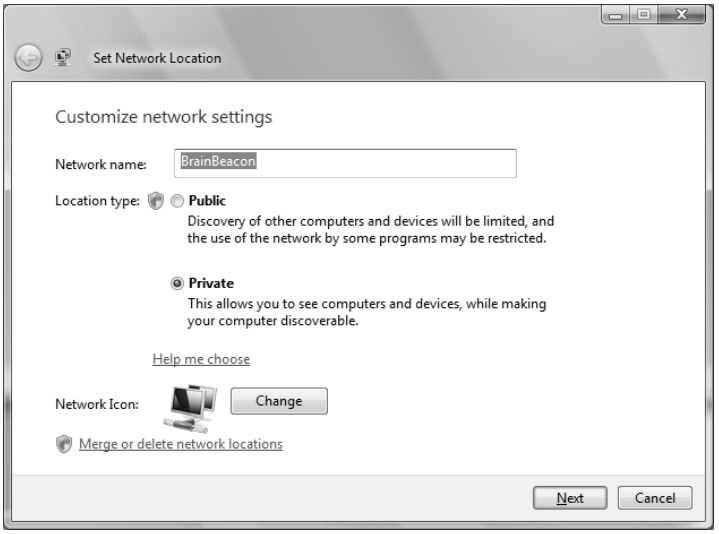


FIGURE 8.12 Set Network Location dialog box



Below the name of the network in the Network and Sharing Center dialog box you can see the Access section, which tells the type of networks to which you are connected. Below that, you can see the Connection type, which specifies the type of network connection you are using. For example, you should see Local Area Connection for a normal, wired network card.

Next to the Connection type, you should see a View Status link. Clicking the View Status link will bring up the Connection Status dialog box for that network connection. From the Connection Status dialog box, shown in Figure 8.13, you can view connection information, including IPv4 and IPv6 status, media state, duration, and the speed at which you connected. You can also see the activity that has been generated for the current session through all packets that have been sent and received through the network adapter. You can also display the adapter's Properties dialog box, disable the adapter, or diagnose the adapter if you are having trouble with it.

If you click the Details button, you will see even more detailed configuration information on your connection in the Network Connection Details dialog box (Figure 8.14).

Public and Private Network Locations

As discussed previously, you can set the network location to Public or Private within the Set Network Location dialog box, shown in Figure 8.12. Setting the network location will automatically configure the Windows Firewall to the appropriate settings for that type of connection.

Setting your network location to Private indicates that you are on a secure, private network. The Private network location allows your computer to discover and connect to other computers and devices, and allows your computer to be discovered by other devices.

Setting your network location to Public indicates that you are on an unsecure, public network. The Public network location prevents your computer from discovering other computers and devices, and limits discovery of your computer by others by disabling the network discovery feature. Additionally, some applications may not be able to fully access the network using this setting.

FIGURE 8.13 The Local Area Connection Status dialog box

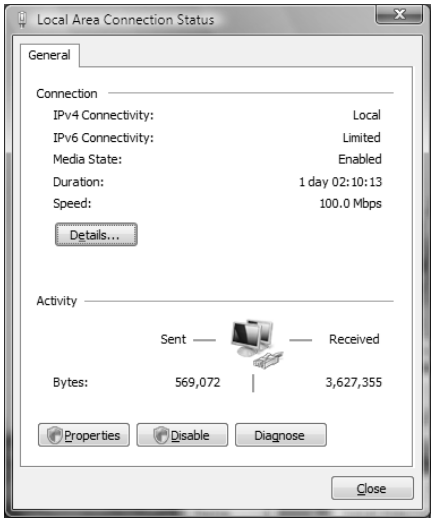
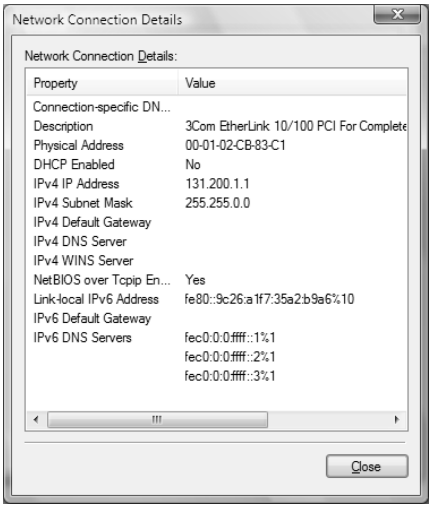


FIGURE 8.14 The Network Connection Details dialog box



If you have a laptop with wireless access, and you use the Private network location setting at home, be sure to switch your network connection to Public when connecting to public wireless access points (WAPs) at places such as airports or restaurants.

Windows Vista also supports a third network location type: Domain. The Domain network location only applies to computers that are members of a corporate domain.

Sharing and Discovery

The Sharing and Discovery section enables you to configure network discovery settings. In addition, you can also configure shared access to files, printers, and media. Each of the sections within Sharing and Discovery have buttons at the end of each row that you can use to open and close the settings within each section; click the button once to open, and again to close.

By default, Windows Vista shares three folders:

- Public
- Users
- Printers

The Public folder can be accessed by anyone on the network, and all users have read and write access. This folder contains Public Documents, Public Downloads, Public Music, Public Pictures, Public Videos, and Recorded TV.

The Users folder contains folders that only authenticated users can access. Each user has their own user folder that they alone can access.

The Printers folder contains printers that are installed on the computer.

Network Discovery

When network discovery is turned on, your computer will be able to detect other network computers and devices, and those computers and devices will also be able to detect your computer as well. In this section, you can turn network discovery on or off.

This section also displays the workgroup or domain to which your computer belongs. A Change Settings link is conveniently placed so that you can easily change your workgroup or domain. Clicking this link will open the System Properties dialog box.

File Sharing

The File Sharing section is used to turn file and printer sharing on and off globally. Turning File Sharing off will also turn Public Folder Sharing and Printer Sharing off.

Public Folder Sharing

The Public Folder Sharing section is used to enable sharing of the Public folder. You can choose from one of the following options:

- Turn on sharing and allow anyone with network access to open files.
- Turn on sharing and allow anyone with network access to open, change, and create files.
- Turn off sharing.

Turning on Public Folder Sharing turns on File Sharing as well.

Even if you turn off Public Folder Sharing, users logged on locally can still access the Public folder.

Printer Sharing

The Printer Sharing section is used to enable sharing of printers installed on the computer. Turning Printer Sharing on turns on File Sharing as well.

Password Protected Sharing

The Password Protected Sharing section is used to configure who should have access to shared files. If Password Protected Sharing is enabled, only users who have an account on the computer can access shared files. If disabled, any user who can connect to the computer can access shared files.

Media Sharing

The Media Sharing section is used to configure access to shared music, pictures, and video. If Media Sharing is enabled, you will allow users to have access to your shared media, and you will be able to locate shared media on other computers. To configure Media Sharing, click the Change button, then select or deselect the check box next to Share My Media.

Tasks

The Tasks pane can be found on the left-hand side of the Network and Sharing Center. You can perform the following tasks:

- View Computers and Devices
- Connect to a Network
- Manage Wireless Networks (only for computers with wireless devices)
- Set Up a Connection or Network
- Manage Network Connections
- Diagnose and Repair

View Computers and Devices

Clicking View Computers and Devices will bring up the Network dialog box, which shows all of the computers and devices on your network. Seeing all of the computers in this manner is much easier than the method used by Windows XP and earlier Windows-based operating systems.

The Network dialog box can also be accessed by selecting Start ➢ Network.

Connect to a Network

Clicking Connect to a Network will display the dial-up, virtual private network (VPN), and wireless networks that have already been created on the computer. You can filter this list so that you are only shown dial-up and VPN connections or only wireless connections by selecting the appropriate group from the Show list.

Manage Wireless Networks

Clicking Manage Wireless Networks will display all of the wireless networks that are configured. We discuss wireless networks later in this chapter.

Set Up a Connection or Network

This feature enables you to set up a new connection. You can set up the following connections:

- Wireless, broadband, or dial-up Internet connection
- Wireless router or access point
- Dial-up or VPN connection to a workplace

We will configure a wireless connection and a VPN connection later in the chapter.

Manage Network Connections

This feature enables you to easily manage your network connections. You have already used this tool earlier in the chapter. To configure a network connection, right-click on the connection and select Properties.

You can bridge network connections by selecting two or more network connections, right-clicking, and selecting Bridge Connections. This is especially useful when connecting a wireless network to a wired network.

Take care when bridging connections. You could expose one network to the security risks of the other network.

Diagnose and Repair

The Diagnose and Repair link runs Windows Network Diagnostics, which automatically checks for any network connectivity problems. Windows Network Diagnostics can detect problems connecting to computers on your wired network, connecting to a wireless access point, or connecting to resources on the Internet. If a problem is found, it will attempt to fix it. You also have the option of reporting the problem to Microsoft.

Introducing Remote Access

When remote users want to access private networks or the Internet, they are faced with a variety of remote access options. You must first have a basic understanding of how remote access works, the connection options associated with remote access, and the security that is used by remote access.

Once you understand the theory behind remote access, you can implement remote access through Windows Vista. To use *dial-up networking*, you need a modem and connections to the remote server or the Internet. You can dial into a Remote Access Service (RAS) server or the Internet, or you can access a VPN server on your network via a connection (for example, through the Internet).

One of the most common ways that remote users can access a private network is through the use of a *Remote Access Service (RAS)* server. The RAS server is used to respond to and

provide services for remote clients. Methods for accessing a RAS server include analog modem and phone system, ISDN adapters and ISDN phone lines, Frame Relay, and leased T lines. The RAS server and the RAS client must use the same connectivity option. They must also use the same protocols as well as compatible security protocols. Figure 8.15 illustrates how you would access a RAS server through analog dial-in service.

A VPN is a private network that uses links across private or public networks (such as the Internet). When data is sent over the remote link, it is encapsulated and encrypted and requires authentication services. You must use Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) to support a VPN connection, both of which are automatically installed on Windows Vista computers. Figure 8.16 illustrates a VPN.

FIGURE 8.15 Dial-in connection to a Remote Access Service (RAS) server

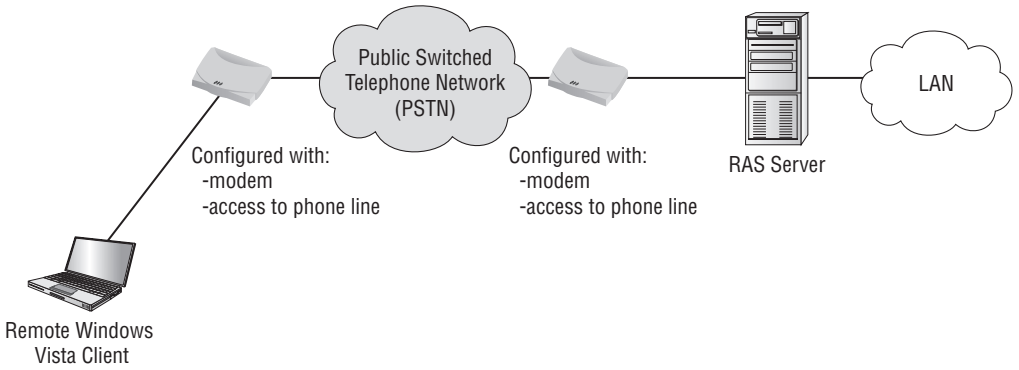
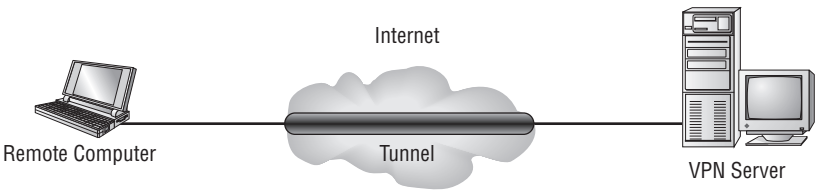


FIGURE 8.16 Making a virtual private network (VPN) connection



In Exercise 8.2, you will configure the client for a VPN connection. This exercise assumes you already have a valid connection to the Internet.

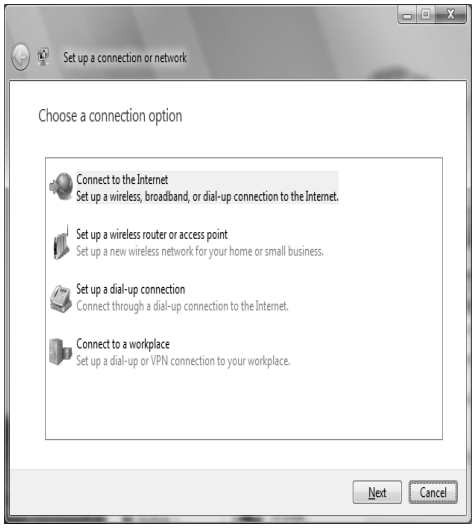
EXERCISE 8.2

Configuring a VPN Client

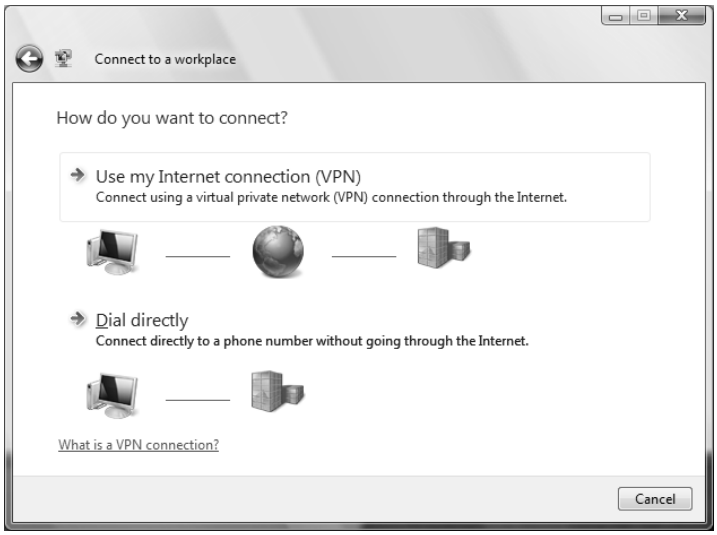
1. Select Start ➢ Network ➢ Network and Sharing Center ➢ Set Up a Connection or Network.

EXERCISE 8.2 *(continued)*

2. The Set Up a Connection or Network dialog box will appear, as shown here. Select Connect to a Workplace, and click Next to continue.

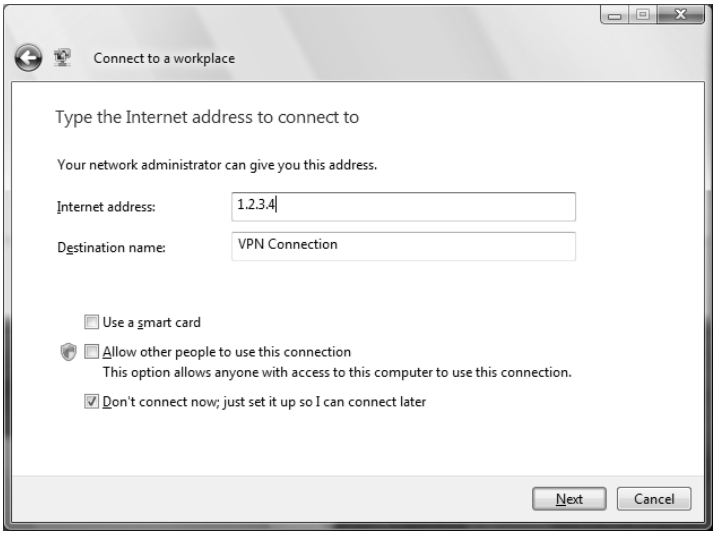


3. The Connect to a Workplace dialog box will appear, as shown here. Select Use My Internet Connection (VPN) and click Next to continue. The Dial Directly option is used to make a dial-in modem connection to a RAS server.

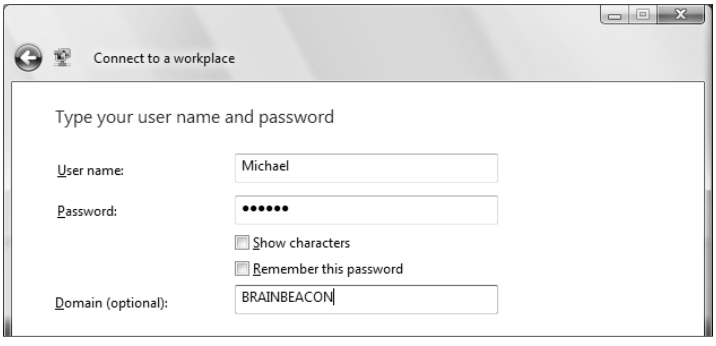


EXERCISE 8.2 *(continued)*

4. Type the IP address of your VPN server at work. If you don't have one, just type **1.2.3.4** in the Internet address field. Then give the connection a name. If smart card authentication is required, select the Use a Smart Card check box. If you want anyone to be able to use this connection, select the Allow Other People to Use This Connection check box; otherwise, only the current user can use the connection. Finally, if you don't want to connect to the VPN server now, select the Don't Connect Now check box. For this scenario, we are selecting the options shown here. Click Next to continue.



5. Type a valid username and password for the VPN server. If you select the Show Characters check box, your password will be displayed; otherwise, it will appear as black dots. Your password will be remembered by Windows Vista if you select the Remember This Password check box. Finally, you can optionally enter the Domain name, as shown here. Click Create to continue.



EXERCISE 8.2 *(continued)*

6. When the connection is ready to use, the screen shown here will be displayed. Click Connect Now to connect, or click Close to finish creating the connection.

7. In the Network and Sharing Center, select Manage Network Connections. You will see your VPN connection displayed in the Network Connections dialog box, as shown here. You can right-click the VPN connection and select Properties to make changes to the connection, such as redial attempts, security settings, type of VPN, and Internet Connection Sharing (ICS).

In the next few sections, we will discuss some of the features that can be configured for remote access connections.

Tunneling Protocols

A *virtual private network (VPN)* is used to provide a remote user with a secure connection to a corporate network via the Internet. Within the VPN, all data to and from the remote access client is encapsulated and encrypted. VPNs are considered a very affordable option for providing high security access between home or small offices over any public network infrastructure that can transport IP packets. The connection methods supported by Windows Vista for use with VPNs include the following:

Point-to-Point Tunneling Protocol The *Point-to-Point Tunneling Protocol (PPTP)* was developed as an open industry standard by Microsoft and other industry leaders to provide support for tunneling of Point-to-Point Protocol (PPP) frames through an IP network. PPP provides authentication, compression, and encryption services. Used in conjunction with Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) and strong passwords, PPTP can provide secure access via a VPN for remote users who use dial-up connectivity to access an Internet service provider (ISP) and from there, the corporate network. This protocol is not considered as secure as L2TP, but it is easier to set up.

Layer Two Tunneling Protocol The *Layer Two Tunneling Protocol (L2TP)* is an industry-standard VPN protocol that is used in conjunction with IP security (IPSec) to provide a high level of security when sending IP packets over the Internet or other public IP network. L2TP and IPSec provide data authentication, data encryption, and data integrity services that strengthen security when data is sent over an unsecured network. In order to use L2TP and IPSec for encryption, User Datagram Protocol (UDP) ports 500 and 1701 must be opened on the corporate network that will be accessed by the remote user.

Authentication Methods

When you access a network through a dial-up connection, VPN, or direct connection, Windows Vista uses a two-step authentication process. The two-step authentication process consists of an interactive logon process and network authorization. The interactive logon process confirms a user's identity based on the user account (local or domain) and password or smart card credentials. Network access control is used to confirm the user's identity to the network service or resource that the user is attempting to access.

To ensure that the interactive logon process is secure over a remote connection, remote authentication protocols can be used. The remote client and the remote network must be configured to negotiate a common remote authentication protocol.

The remote authentication protocols that are supported by Windows Vista are as follows:

Password Authentication Protocol *Password Authentication Protocol (PAP)* is the simplest authentication method. It uses unencrypted, plain-text passwords. You would use PAP if the server you were connecting to didn't support secure validations or you were troubleshooting remote access and wanted to use the most basic authentication option.

Don't use PAP if security is important to you. PAP sends passwords in clear text.

Challenge Handshake Authentication Protocol *Challenge Handshake Authentication Protocol (CHAP)* is used to negotiate secure authentication by using encryption that is based on the industry-standard hashing scheme specified by Message Digest 5 (MD5). Hashing schemes are used to transform data into a scrambled format. CHAP uses a challenge-response process that sends the client a request with the hash scheme that will be used. The client then responds to the server with an MD5 hashed response. This method allows the server to authenticate a client without the client actually sending their password over the remote connection. Almost all third-party PPP servers support CHAP authentication.

Microsoft Challenge Handshake Authentication Protocol Version 2 *Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)* adds to the services provided by CHAP by providing mutual authentication, different encryption keys for sending and receiving, and stronger data encryption keys. Windows 2000 (all versions), Windows XP (all versions), Windows Vista (all versions), and Windows Server 2003 can use MS-CHAPv2 with dial-up and VPN connections. If you are using Windows NT 4 (all versions) or Windows 95/98 computers, you can use only MS-CHAPv2 authentication with VPN connections.

When MS-CHAPv2 is used to authenticate, your connection can be configured to automatically use your Windows username, password, and domain settings.

Extensible Authentication Protocol *Extensible Authentication Protocol (EAP)* extends the services of PPP by providing more updated and secure authentication services than were previously available with PPP. EAP was designed to provide secure authentication services for third-party (non-Microsoft) devices. You can smart card authentication or certificate authentication with EAP. You can also use Protected EAP (PEAP) to authenticate with EAP-MSCHAPv2, smart card, or certificate.

Smart cards are small credit-card-sized devices that are used with a smart card reader to provide an additional level of hardware security.

Certificate authentication uses a special authentication credential, called a certificate. A certificate is a digital signature that is issued by a certification authority. When a client and server are configured to use certificate authentication, they must both present a valid certificate for mutual authentication.

Encryption Options

Data encryption adds an additional layer of security by encrypting all of the data that is sent through a remote connection in addition to adding security to the logon authentication process. If you are using Windows Vista to create a remote connection with dial-up, VPN, or remote connections, there are two options for using data encryption (both options support multiple key strengths that can be applied to data encryption):

Microsoft Point-to-Point Encryption PPTP does not itself provide encryption, so it relies on *Microsoft Point-to-Point Encryption (MPPE)* to provide it. MPPE is a PPP data encryption option that uses Rivest-Shamir-Adleman (RSA) RC4 encryption. MPPE supports strong (128-bit key) or standard (40-bit key) encryption. In order to use MPPE data encryption over a dial-up or VPN connection, the remote client and server that will be accessed must use the MS-CHAPv2 or EAP authentication protocols.

IPSec L2TP uses *Internet Protocol Security (IPSec)* for computer-level authentication and encryption of VPN connections. IPSec uses Data Encryption Standard (DES) encryption. IPSec services include packet data authentication, data integrity, replay protection, and data confidentiality services.

If the remote client and remote network use PAP or CHAP for authentication, you will not have the option to use data encryption for dial-up and PPTP connections.

Remote Access Troubleshooting

Here are some tips you can use if you have trouble establishing a remote access session to a RAS or VPN server:

- Ensure your modem's phone line or your network connection to the Internet is working. Use Diagnose and Repair to help fix a connection.
- Ensure that the VPN connection is configured with the correct VPN server IP address, username, and password.
- Ensure that both sides of the connection are configured to use a common authentication protocol.
- Ensure that both sides of the connection have compatible encryption requirements. For example, if the server requires encryption, and the client is set to offer no encryption, then the connection will not be established.
- Ensure that both sides of the connection are set to use the same tunneling protocol. Windows Vista supports using Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP).

Connecting to Network Devices

You can configure Windows Vista to connect to many types of networked devices, including network projectors and printers. We will discuss how to configure Windows Vista to use these devices.

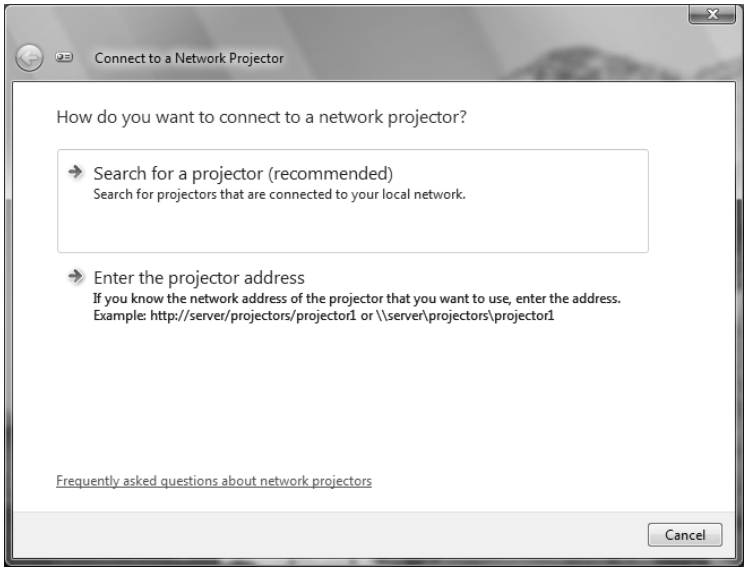
Network Projectors

Windows Vista includes network projector support. If the projector is configured properly on your wired or wireless network, you can use it as a networked display. To set up a network projector, select Start ➢ All Programs ➢ Accessories ➢ Connect to a Network Projector. The Connect to a Network Projector dialog box, shown in Figure 8.17, will appear.

Click Search for a Projector to search for a projector that is connected to your wired or wireless network. If no projectors are found, but you know the IP address or network name of the projector, select Enter the Projector Address. You will also need the password of the projector if it is configured with one.

Network projector support is not included in Windows Vista Home Basic.

FIGURE 8.17 Connect to a Network Projector

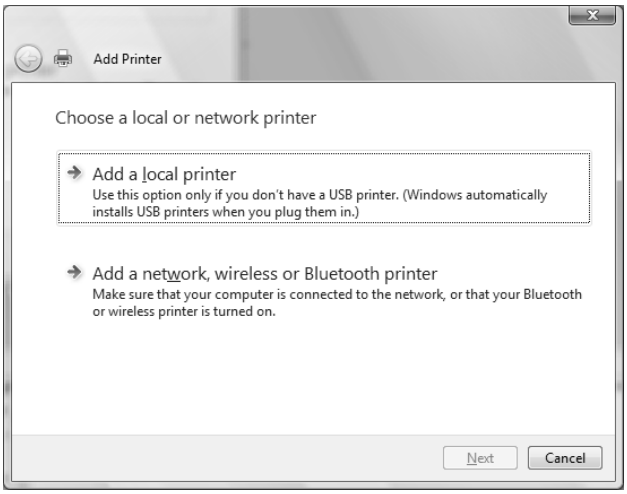


Network Printers

Adding a network printer to Windows Vista is much easier than it was in previous versions of Windows. To add a network printer, select Start ➢ Control Panel ➢ Printers. When the Printers dialog box is displayed, click Add a Printer. The Add Printer dialog box, shown in Figure 8.18, will be displayed.

To add a network printer, select Add a Network, Wireless or Bluetooth Printer. Windows Vista will search for available printers and allow you to install them. If your printer isn't found, you can select The Printer That I Want Isn't Listed and browse for a printer, or you can select a printer by name or IP address.

FIGURE 8.18 Add Printer dialog box



Supporting Wireless Network Connections

As wireless technology matures and has become cost effective, the use of wireless network adapters is increasingly popular. Windows Vista supports wireless autoconfiguration, which makes wireless network connections easy to use. Windows Vista automatically selects the wireless networks that it finds and attaches you to the preferred network. In the following sections you will learn how to configure your wireless network settings and how to secure a wireless network in a small or home network.

Configuring Wireless Network Settings

If you have a wireless network adapter (either a network card that you add to your computer or an adapter that is built into your computer) and it is designed to work with Windows Vista, it will be automatically recognized by the operating system. You can see the wireless network adapter by selecting Start ➢ Network ➢ Network and Sharing Center ➢ Manage Network Connections. A sample wireless network adapter is shown in the Network Connections window in Figure 8.19.

When you right-click a wireless adapter and click Properties, you see the Wireless Network Connection Properties dialog box, shown in Figure 8.20. The General Properties tab is similar to what you would see with a normal network adapter. Click OK to close the dialog box.

You can connect to a wireless network in a couple of different ways. First, you can right-click the Wireless Network Connection and select Connect / Disconnect. The resulting dialog box lists all of the wireless networks that are detected, as shown in Figure 8.21, and shows the wireless network name, whether it is unsecured or security-enabled, and the connection strength. If you mouse over a wireless network listing, you can also see the type of security and wireless protocol that it uses. To connect, select a network by highlighting it and then clicking the Connect button in the lower-right corner of the dialog box. You can also select Set Up a Connection or Network to manually connect to a wireless network.

FIGURE 8.19 Network Connections window

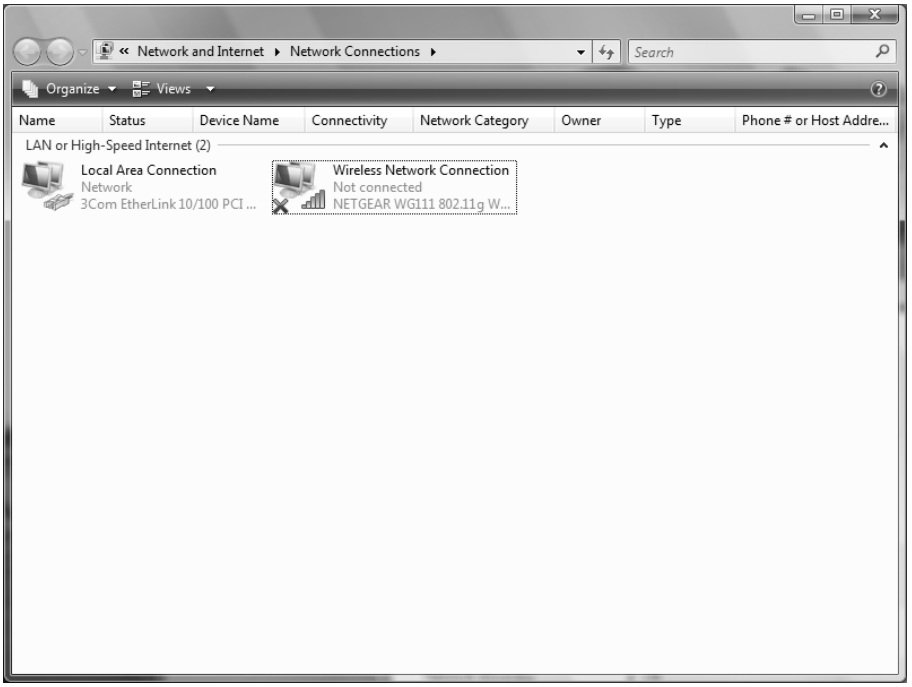


FIGURE 8.20 Wireless Network Connection Properties dialog box

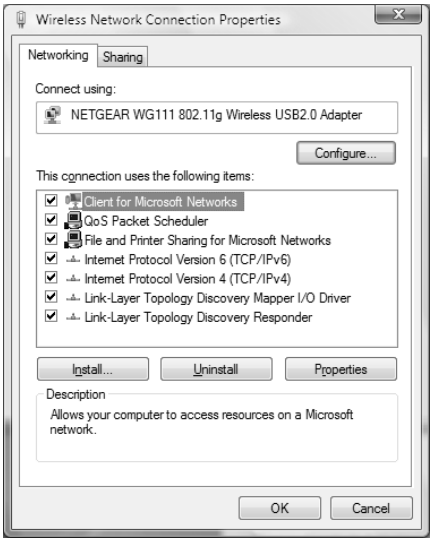
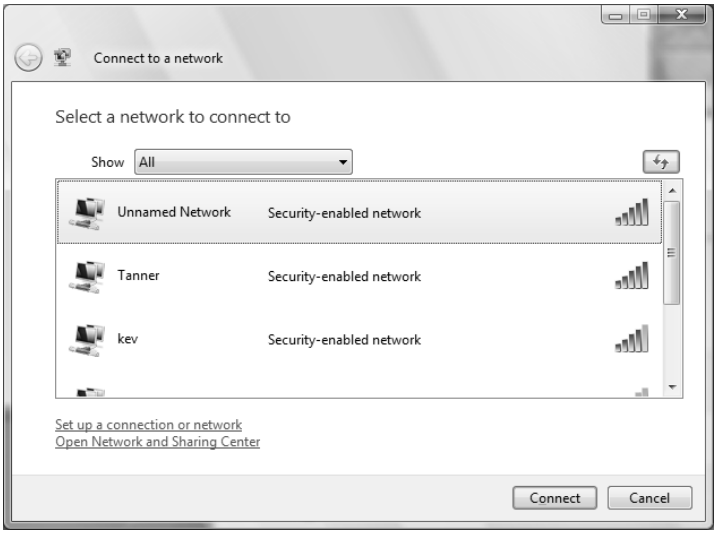


FIGURE 8.21 Connect to a Network dialog box



If the network name is listed as "Unnamed Network", you will be asked for the network name, or SSID (Service Set Identifier). If security exists on the wireless network, you will also be prompted for the security key or passphrase, as shown in Figure 8.22. If the key is correct, you will be connected to the wireless network.

To manually connect to a wireless network, right-click your Wireless Network Connection and select Connect / Disconnect to get back to the Connect to a Network dialog box. At the bottom of the page, select Set Up a Connection or Network. In the Choose a Connection Option dialog box, you can set up a wireless router or access point, or configure an ad hoc wireless network, which is a computer-to-computer network that doesn't require a wireless router. However, we want to select Manually Connect to a Wireless Network, as shown in Figure 8.23.

From here, you will be prompted for the network name, type of security used, type of encryption used, and the security key or passphrase, as shown in Figure 8.24. You can also choose whether to start the connection automatically, or to start it regardless of whether the wireless network is available. After you enter the information and click Next, the network will be added and you can choose to connect or change the settings.

You can manage your wireless network connections by clicking Start ➢ Network ➢ Network and Sharing Center ➢ Manage Wireless Networks. As shown in Figure 8.25, you can see each of the networks you have added, along with the security type, network type, and whether you will automatically connect. You can add or remove a wireless network connection, rename a connection, or move an existing connection up or down to give it a higher or lower priority. Your wireless adapter will connect to the wireless network with the highest priority before connecting to those with lower priority.

FIGURE 8.22 Network security key or passphrase

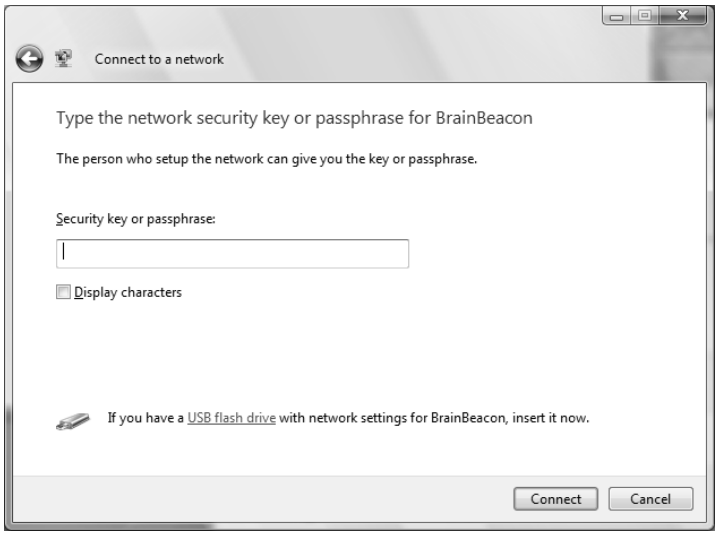


FIGURE 8.23 Choosing a connection option

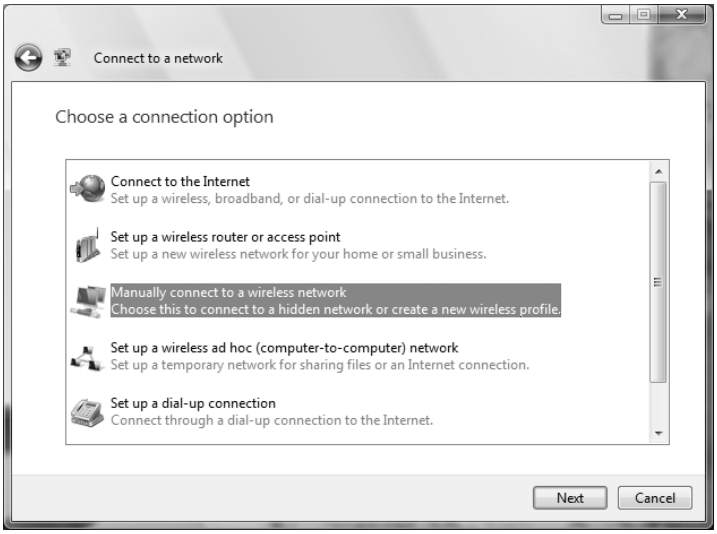


FIGURE 8.24 Manually Connect to a Wireless Network window

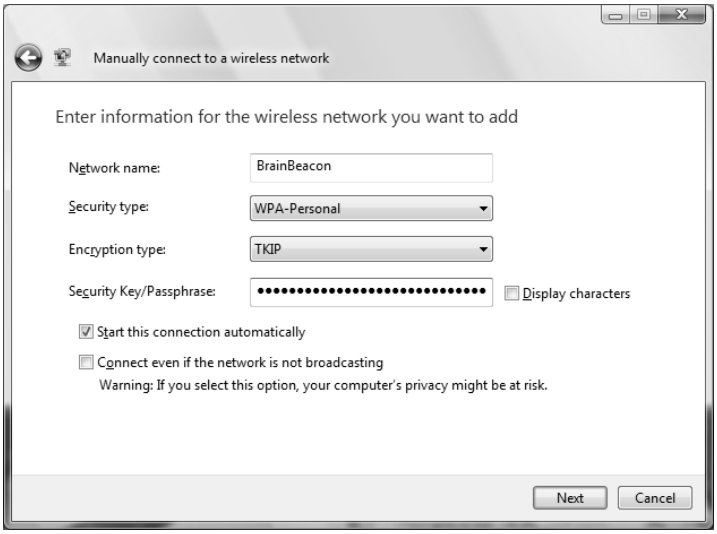
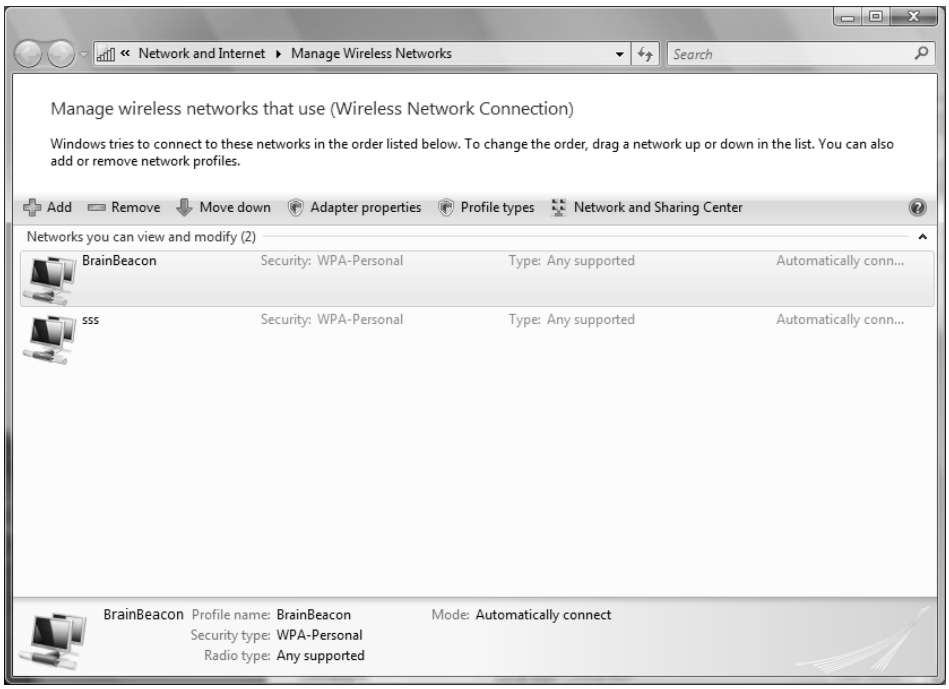


FIGURE 8.25 Manage Wireless Networks window



Your computer will automatically connect to the network that is highest on the list. To change the network priority, select the wireless network and click Move Up or Move Down.

Clicking Adapter Properties will bring up the Wireless Adapter Properties dialog box, as shown previously in Figure 8.20. The Profile Types option is used to specify whether wireless connections should be configured for all users or only for the user who creates the connection. Finally, Network and Sharing Center will take you back to the Network and Sharing Center dialog box.

If a user configures a wireless network connection on a shared computer, the wireless connection may not be available to other users. To make the connection available to all users, click Profile Types and selecting Use All-User Profiles Only. Selecting the Use All-User and Per-User Profiles option allows users to create wireless connections that only they can access.

Double-clicking on a wireless network will bring up the Wireless Network Properties dialog box, as shown in Figure 8.26. The Connection tab shows the network name and SSID, the network type, the network availability, and other connectivity options.

To ensure that your computer connects automatically when the wireless network is in range, be sure that you select the check box next to Connect Automatically When This Network Is in Range.

If you select Connect to a More Preferred Network if Available, then your computer will first try to connect to wireless networks that are higher in priority (shown in Figure 8.25) before connecting to this network.

To be sure that you can connect to a network that is not broadcasting its SSID, select Connect Even if the Network Is Not Broadcasting.

The Security tab of the Wireless Network Properties dialog box is shown in Figure 8.27. Here, you can modify the security type, the encryption type, and the security key or passphrase.

Configuring Security for a Small Wireless Network

Even in a small wireless network, you should still configure network security. There are three things that you can do to increase the security of a wireless network:

- Disable broadcast of the SSID, which is the name of the wireless network. When SSID broadcast is disabled, the wireless network cannot be detected automatically until you manually configure your wireless network card to connect to that SSID.

FIGURE 8.26 Wireless Network Properties

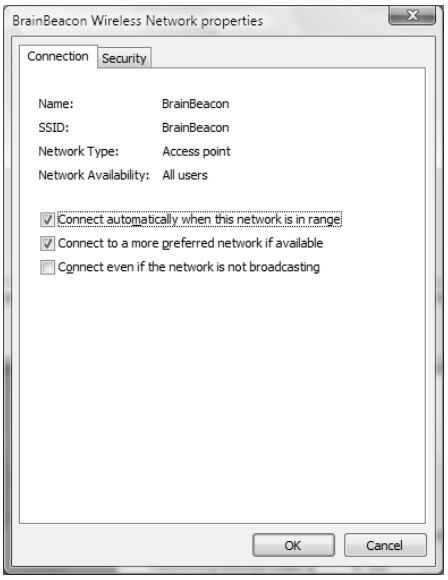
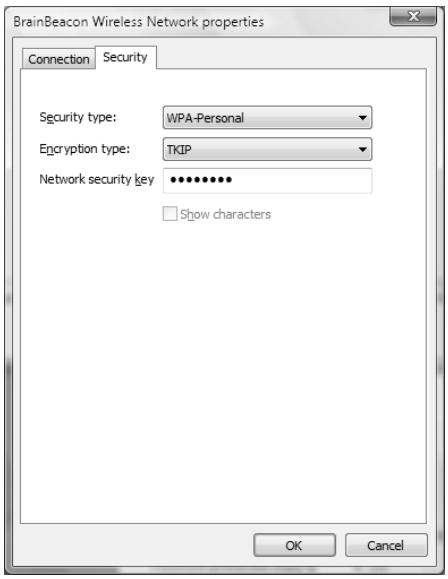


FIGURE 8.27 Security tab of Wireless Network Properties



- Create a Media Access Control (MAC) address filter list so that only wireless devices with specific hard-coded MAC addresses are allowed to connect.
- Enable encryption, such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2.

Use WPA or, preferably, WPA2 whenever possible. WEP encryption is extremely easy for intruders to decrypt.

You can easily set up a secure wireless network by using the Wireless Network Setup Wizard, as shown in the following steps:

1. From the Choose a Connection Option dialog box (shown in Figure 8.23), select Set Up a Wireless Router or Access Point.
2. The Wireless Network Setup Wizard will start. Click the Next button.
3. The wizard might ask whether you want to turn on network discovery for public networks. After you make your selection, the wizard will detect your hardware and settings.

4. If Windows can connect to the wireless router and configure it automatically, it will prompt you through the appropriate steps. However, if Windows cannot configure it automatically, you can configure the device manually using a web browser or configure the settings and save them to a USB flash drive, as shown in Figure 8.28. However, to use the USB flash drive option, you must have a wireless device that supports it.
5. If you select the Configure This Device Manually option, a web browser will open so that you can configure the wireless router. You will most likely be prompted for a username and password. If you authenticate successfully, you will be taken to the wireless router's web interface. Follow the instructions in the router's manual.
6. If you select the Create Wireless Settings and Save to USB Flash Drive option, you will be asked to create an SSID for your network, as shown in Figure 8.29. Click Next to continue.
7. In the Help Make Your Network More Secure With a Passphrase screen, shown in Figure 8.30, you can enter a passphrase to use for your network, which will be converted to a Wi-Fi Protected Access (WPA) security key. If you want to be able to choose the security method used, select Show Advanced Security Options. After you have created your passphrase, click Next.
8. In the Choose File and Printer Sharing Options screen, shown in Figure 8.31, you can select how printers and files are shared on your network. Click Next to continue.
9. You are prompted to insert the USB flash drive into your computer, as shown in Figure 8.32. Select the flash drive you want to use and click Next.

FIGURE 8.28 Wireless router configuration

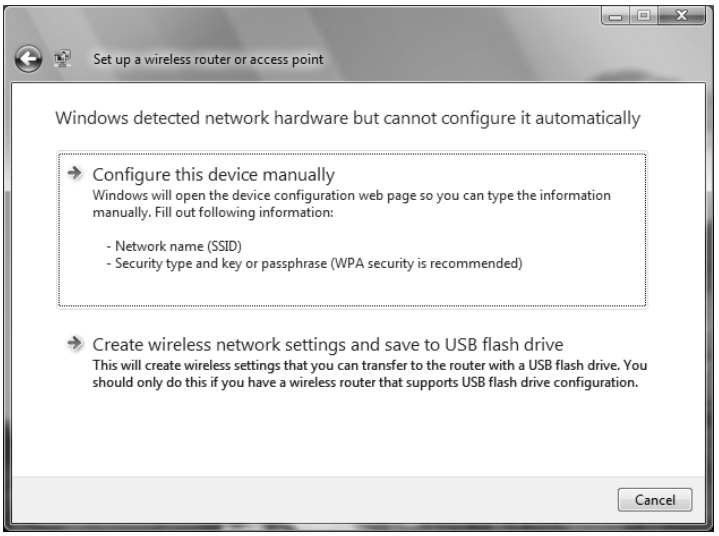


FIGURE 8.29 The Give Your Network a Name screen

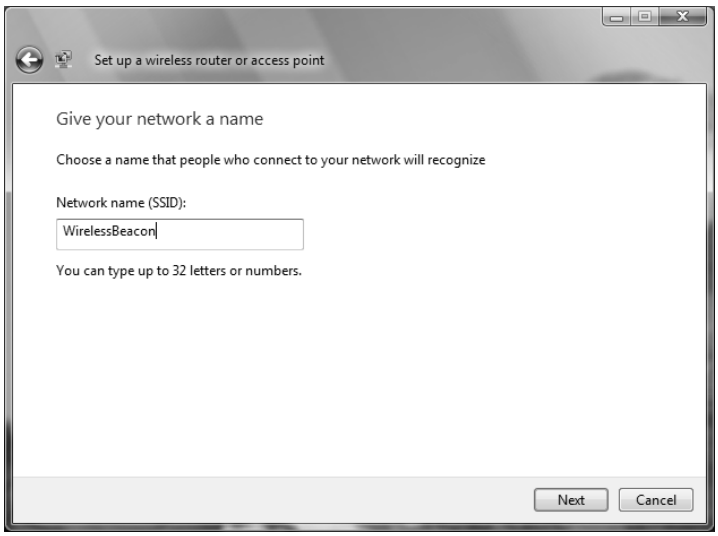


FIGURE 8.30 Help Make Your Network More Secure With a Passphrase screen

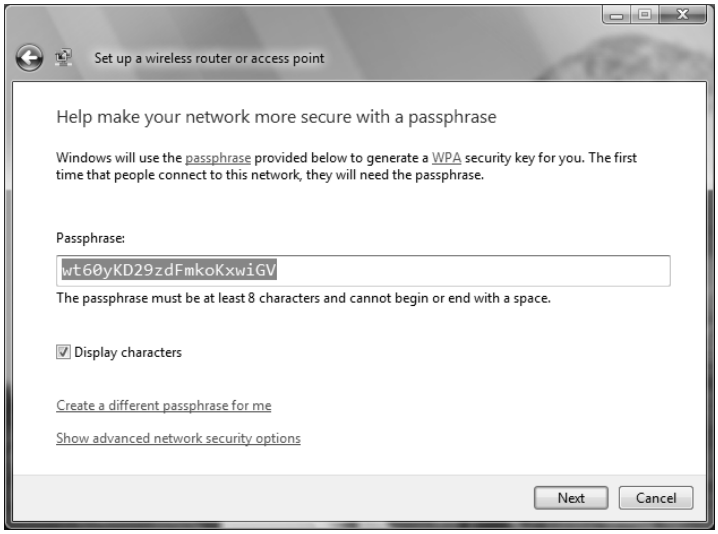


FIGURE 8.31 Choose File and Printer Sharing Options screen

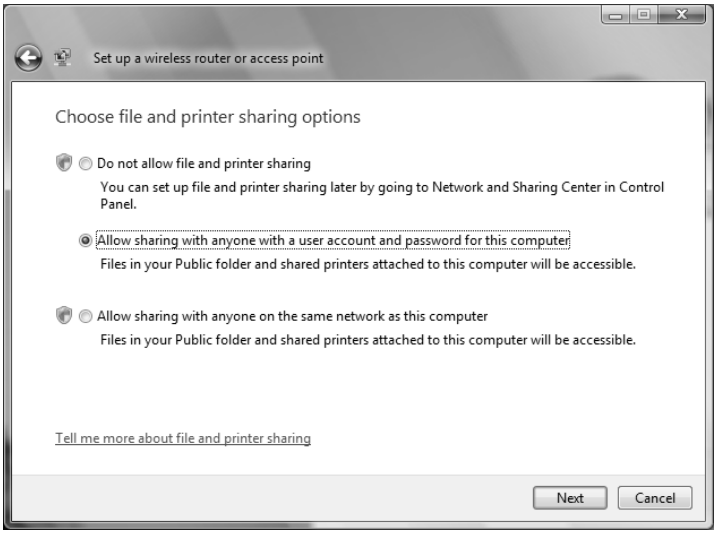


FIGURE 8.32 Insert the USB Flash Drive dialog box

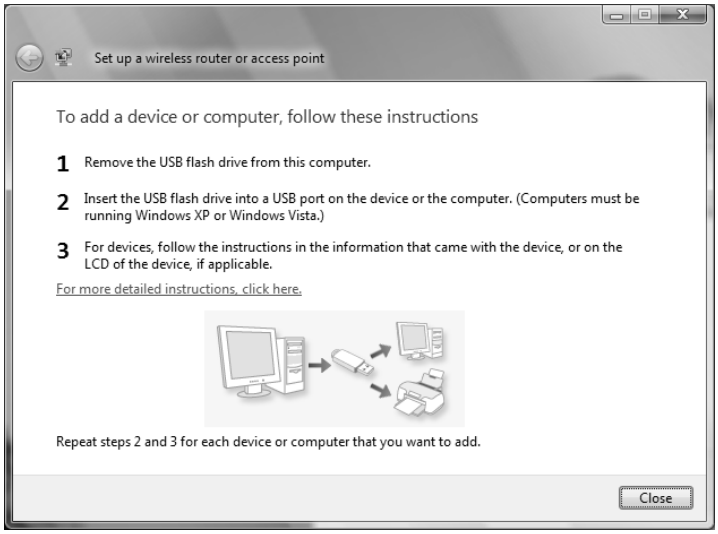
10. Data will be copied to the flash drive. After the data has been copied, you will be given instructions on how to copy the saved settings to another computer or to a wireless router, as shown in Figure 8.33. Click Close to close the screen. The wireless network will be added to your saved networks.

The flash drive will contain a few files, including `setupSNK.exe`, which launches the Wireless Network Setup Wizard. This is used to roll out the wireless network settings to other computers.

Be sure to safeguard this USB key! Not only does it contain the application to automatically configure Windows-based devices for your wireless network, it also contains two files, `WSETTING.TXT` and `SETTING.WFC`, within the `SMRTNTKY` folder. These files contain the SSID and security key for your network, all stored in clear text.

11. To configure another computer with the wireless network, simply insert the USB flash drive into the computer. If the Wireless Network Setup Wizard (`setupSNK.exe`) does not launch automatically, you should manually launch it by browsing to the drive and double-clicking `setupSNK.exe`. This application is compatible with Windows XP with SP2 and Windows Vista.

FIGURE 8.33 To Add a Device or Computer screen



Real World Scenario

Rolling Out Wireless Configurations to Multiple Computers

Let's say you've got a network with hundreds or thousands of Windows Vista and Windows XP (SP2) computers that you want to configure with wireless network settings. Certainly you wouldn't want to visit each computer individually and manually configure those settings. Luckily, as we've seen in the previous section, you can copy the wireless settings to a USB key.

But do you still have to visit each computer and manually insert the USB key to copy the settings? That would be awfully cumbersome. Fortunately, there is another option. You can copy the contents of the USB key to a shared location on the network. Then, you can configure a login script (which is easy to distribute using Group Policy) that will map the shared folder to a drive letter and run `setupSNK.exe`.

Note that `setupSNK.exe` must be run from a mapped drive or it will not launch. You can't run it from a folder on your hard drive or directly from a shared folder without first mapping a drive to it.

Alternatively, you can copy the files to a CD or DVD and distribute them. When the CD or DVD is inserted, the Wireless Network Setup Wizard will launch automatically if Autoplay is enabled. This solution is helpful for computers that do not already have connectivity to a shared network location. However, for computers that can access a shared network location, using a shared folder with a login script is by far the easiest distribution method.

Troubleshooting Wireless Connectivity

If you are having problems connecting to a wireless network, here are some things you can try:

- Ensure that your wireless network card is enabled. Many newer laptops and tablets have either a switch or a hot-key setting that enables and disables the wireless device.
- Ensure that the access point is turned on and that you are close enough to it.
- Ensure that there is nothing that might be causing interference of the wireless signal.
- Ensure that the SSID, encryption type, and passphrase/security key are correct.
- Ensure that your wireless card and the access point are compatible. Cards that are compatible with the 802.11b standard can only connect to 802.11b access points, and cards using 802.11a can only connect to 802.11a access points. However, 802.11g cards can connect to either 802.11g or 802.11b access points.
- If you are having trouble connecting to a network that does not broadcast its SSID, select the Connect Even if the Network Is Not Broadcasting check box in the Wireless Network Properties dialog box (shown in Figure 8.26).

Overview of Network Protocols

Network protocols function at the Network and Transport layers of the OSI model. They are responsible for transporting data across an internetwork. Only TCP/IP is installed with Windows Vista by default.

Previous versions of Windows also supported a protocol called NetBEUI. NetBEUI is a very easy protocol to install and requires no configuration. However, it does not offer as many networking features as TCP/IP. Microsoft discontinued support of NetBEUI with Windows XP.

Overview of TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most commonly used network protocol. It is a suite of interconnected protocols that have evolved as the industry standard for network, internetwork, and Internet connectivity. The main protocols that provide basic TCP/IP services include Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).

The following sections describe the benefits and features of TCP/IP, as well as the basics of TCP/IP addressing.

Benefits of Using TCP/IP

On a clean installation of Windows Vista, TCP/IP is installed by default. TCP/IP has the following benefits:

- TCP/IP is the most common protocol and is supported by almost all network operating systems. It is the required protocol for Internet access.
- TCP/IP is dependable and scalable for use in small and large networks.
- Support is provided for connectivity across interconnected networks, independent of the operating systems being used. TCP/IP provides connectivity for operating systems such as IBM mainframes, Apple Macintosh, Unix and Linux systems, and Open Virtual Memory Systems (VMS).
- TCP/IP provides standard routing services for moving packets over interconnected network segments. Dividing networks into multiple subnets optimizes network traffic and facilitates network management.
- TCP/IP is designed to be fault tolerant. It is able to dynamically reroute packets if network links become unavailable (assuming alternate paths exist).
- Protocol companions such as *Dynamic Host Configuration Protocol (DHCP)* and Domain Name System (DNS) offer advanced functionality.

- Support for *Automatic Private IP Addressing (APIPA)*, which is used by small networks without a DHCP server to automatically assign themselves IP addresses, is included.
- Support for *NetBIOS* over TCP/IP (NetBT) is included. NetBIOS is used for identifying computer resources by name as opposed to IP address.
- Performance enhancements include a larger TCP receive window for more efficient communication.
- The inclusion of *Alternate IP Configuration* allows users to have a static and a DHCP-assigned IP address mapped to a single network adapter, which is used to support mobile users who roam between different network segments.

Features of TCP/IP

One of the main features of TCP/IP is that it allows a common structure for network communications across a wide variety of diverse hardware and operating systems. For example, the underlying hardware could be 10Mbps Ethernet, 100Mbps Ethernet, or Token Ring. The computer operating systems that commonly use TCP/IP are Windows operating systems, Unix, Linux, and NetWare. TCP/IP provides a common network access method independent of the hardware and operating systems used.

The features of TCP/IP included with Windows Vista are as follows:

- Logical and physical multihoming, which allows you to have multiple IP addresses on a single computer for single or multiple network adapters. Multiple network adapters installed on a single computer are normally associated with routing for internetwork connectivity.
- Support for internal IP routing, which allows a Windows Vista computer to route packets between multiple network adapters that have been installed.
- The ability to support multiple default network gateways, which are associated with network routing.
- Support for virtual private networks, which allow you to transmit data securely across a public network via encapsulated and encrypted packets.
- Network and Sharing Center, which allows you to browse network resources even if they are located on a remote subnet.
- Use of a NetBIOS interface, which supports NetBIOS sessions, datagrams, and name management via TCP/IP.
- Inclusion of a Simple Network Management Protocol (SNMP) agent that can be used to monitor performance and resource use of a TCP/IP host.
- TCP/IP connectivity tools added for allowing access to heterogeneous hosts across a TCP/IP network. Connectivity tools include FTP, TFTP, Telnet, and finger.
- TCP/IP management and diagnostic tools included for providing maintenance and diagnostic support. TCP/IP management and diagnostic commands include `ipconfig`, `arp`, `ping`, `nbtstat`, `netsh`, `route`, `nslookup`, `tracert`, and `pathping`.
- Support for TCP/IP network printing, which allows you to print to networked print devices.

Basics of IP Addressing and Configuration

Before you can configure TCP/IP, you must have a basic understanding of TCP/IP configuration and addressing. To configure a TCP/IP client, you must specify an IP address and subnet mask. Depending on your network, optional settings might include the default gateway, DNS server settings, and WINS server settings.

In the following subsections, you will learn about these TCP/IP addressing and configuration options:

- IP address
- Subnet mask
- Default gateway
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS) servers
- Windows Internet Name Service (WINS) servers

In the section "Options for Deploying TCP/IP Configurations," you will learn about the four methods that can be used to implement TCP/IP addressing and configuration.

IPv4 Address

The *IP address* uniquely identifies your computer on the network. The IP address scheme used by the Internet is Internet Protocol version 4 (IPv4). An IPv4 address is a four-field, 32-bit address, separated by periods (an example is 165.76.21.22). Part of the address is used to identify your network address, and part is used to identify the host (or local) computer's address.

There are three main classes of IP addresses. Depending on the class you use, different parts of the address show the network portion of the address and the host address, as illustrated in Figure 8.34.

FIGURE 8.34 IP class network and host addresses

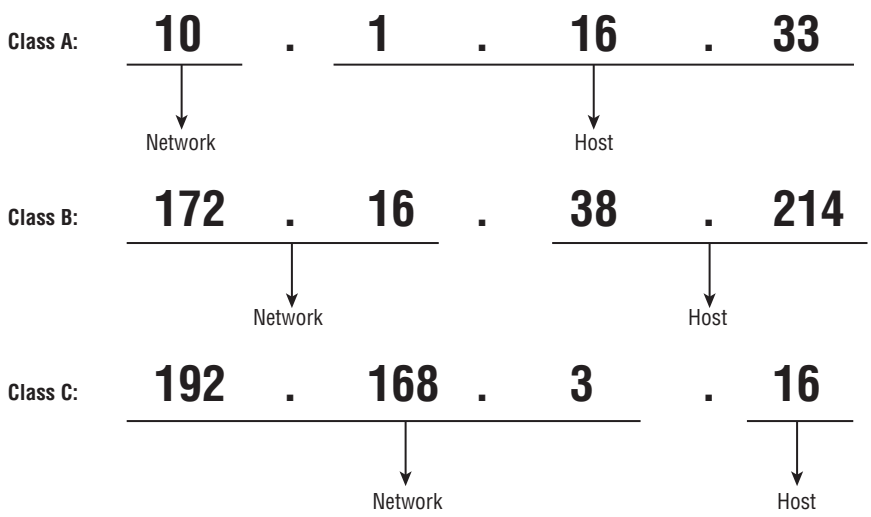


Table 8.1 shows the three classes of network addresses and the number of networks and hosts that are available for each network class.

Addresses beginning with 127 are used for diagnostic and troubleshooting purposes. For example, the address 127.0.0.1 is commonly known as the loopback address, and is used to determine whether IP is working properly on your computer.

TABLE 8.1 IP Class Assignments

Network Class	Address Range of First Field	Number of Networks Available	Number of Host Nodes Supported Per Network
A	1–126	126	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254

Subnet Mask

The *subnet mask* is used to specify which part of the IP address is the network address and which part of the address is the host address. By default, the following subnet masks are applied:

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

By using 255, you are selecting the octet or octets (or, in some cases, the piece of an octet) used to identify the network address. For example, in the Class B network address 191.200.2.1, if the subnet mask is 255.255.0.0, then 191.200 is the network address and 2.1 is the host address.

When a network administrator is designing the network infrastructure, the creation and administration of subnet masks can be a difficult task. For more detailed information on subnet masks, see *MCSE: Windows Server 2003 Network Infrastructure Planning and Maintenance Study Guide (70-293)* (Sybex, 2003).

Default Gateway

You configure a *default gateway* if the network contains routers. A *router* is a device that connects two or more network segments together. Routers function at the Network layer of the OSI model.

You can configure a Windows Vista computer or a Windows Server 2003 computer to act as a router by installing two or more network cards in the server, attaching each network card to a different network segment, and then configuring each network card for the segment to which it will attach. You can also use third-party routers, which typically offer more features than Windows Vista computers or Windows Server 2003 computers configured as routers.

As an example, suppose that your network is configured as shown in Figure 8.35. Network A uses the IP network address 131.1.0.0. Network B uses the IP network address 131.2.0.0. In this case, each network card in the router should be configured with an IP address from the segment to which the network card is addressed.

You configure the computers on each segment to point to the IP address of the network card on the router that is attached to their network segment. For example, in Figure 8.35, the computer VISTA1 is attached to Network A. The default gateway that would be configured for this computer is 131.1.0.10. The computer VISTA2 is attached to Network B. The default gateway that would be configured for this computer is 131.2.0.10.

DHCP

Each device that will use TCP/IP on your network must have a valid, unique IP address. This address can be manually configured or can be automated through *Dynamic Host Configuration Protocol (DHCP)*. DHCP is implemented as a DHCP server and a DHCP client, as shown in Figure 8.36. The server is configured with a pool of IP addresses and other IP-related configuration settings. The client is configured to automatically access the DHCP server to obtain its IP configuration.

FIGURE 8.35 Configuring default gateways

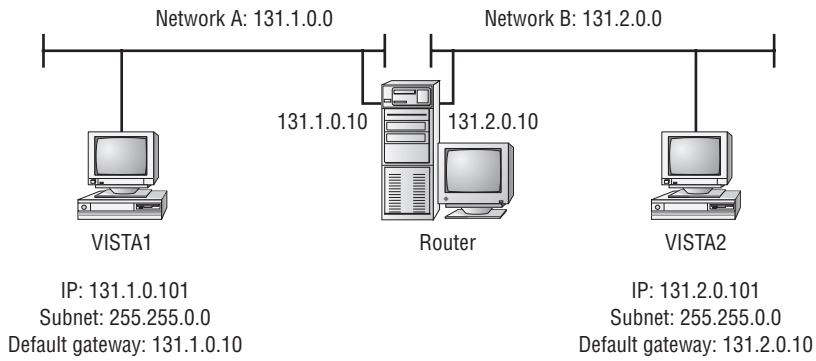
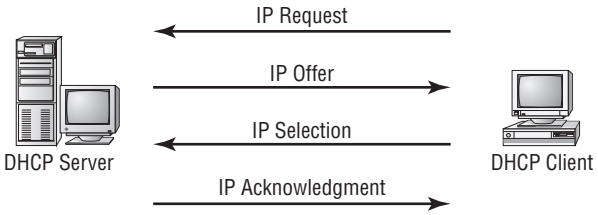


FIGURE 8.36 The DHCP lease-generation process



DHCP works in the following manner:

1. When the client computer starts up, it sends a broadcast DHCPDISCOVER message, requesting a DHCP server. The request includes the hardware address of the client computer.
2. Any DHCP server receiving the broadcast that has available IP addresses will send a DHCPOFFER message to the client. This message offers an IP address for a set period of time (called a *lease*), a subnet mask, and a server identifier (the IP address of the DHCP server). The address that is offered by the server is marked as unavailable and will not be offered to any other clients during the DHCP negotiation period.
3. The client selects one of the offers and broadcasts a DHCPREQUEST message, indicating its selection. This allows any DHCP offers that were not accepted to be returned to the pool of available IP addresses.
4. The DHCP server that was selected sends back a DHCPACK message as an acknowledgment, indicating the IP address, subnet mask, and duration of the lease that the client computer will use. It may also send additional configuration information, such as the address of the default gateway and the DNS server address.

If you want to use DHCP and there is no DHCP server on your network segment, you can use a DHCP server on another network segment—provided that the DHCP server is configured to support your network segment and that a DHCP Relay Agent has been installed on your network router.

If you are not able to access a DHCP server installed on a Windows 2000 Server or Windows Server 2003 within Active Directory, make sure that the DHCP server has been authorized.

DNS Servers

Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. This makes it easier for people to access domain hosts. For example, do you know what the IP address is for the White House? No? Do you know the domain hostname of the White House? You probably guessed that it's `www.whitehouse.gov`. You can understand why many people might not know the IP address but would know the domain hostname.

When you access the Internet and type in **`www.whitehouse.gov`**, there are DNS servers within the infrastructure of the Internet that resolve the hostname to the proper IP address. If you do not have access to a properly configured DNS server, you can configure a `HOSTS` file for your computer that contains the mappings of IP addresses to the domain hosts that you need to access.

If you can access a computer by IP address but not by name, you've probably got a DNS resolution problem.

WINS Servers

Windows Internet Name Service (WINS) servers are used to resolve NetBIOS (Network Basic Input/Output System) names to IP addresses. Windows Vista uses NetBIOS names in addition to hostnames to identify network computers. This is mainly for backward compatibility with Windows NT 4, which used this addressing scheme extensively. When you attempt to access a computer using the NetBIOS name, the computer must be able to resolve the NetBIOS name to an IP address. This address resolution can be accomplished by using one of the following methods:

- Through a broadcast (if the computer you are trying to reach is on the same network segment)
- Through a WINS server
- Through an `LMHOSTS` file, which is a static mapping of IP addresses to NetBIOS computer names

Name resolution is covered in greater detail in the "Understanding TCP/IP Name Resolution" section of this chapter.

Options for Deploying TCP/IP Configurations

Windows Vista offers four methods for configuring TCP/IP. You can use Dynamic Host Configuration Protocol (DHCP), Automatic Private IP Addressing (APIPA), Static IP Addressing, or Alternate IP Configuration. The following sections include a description of each option, as well as instructions for configuring each option.

Using DHCP

Dynamic IP configuration assumes that you have a DHCP server on your network. DHCP servers are configured to automatically provide DHCP clients with all their IP configuration information, including IP address, subnet mask, and DNS server. For large networks, DHCP is the easiest and most reliable way of managing IP configurations. By default, when TCP/IP is installed on a Windows Vista computer, the computer is configured for dynamic IP configuration.

If your computer is configured for manual IP configuration and you want to use dynamic IP configuration, take the following steps:

1. Select Start ➢ Network ➢ Network and Sharing Center.
2. In the Network and Sharing Center dialog box, click the Manage Network Connections option. You will see your Local Area Connection as an icon.
3. Right-click Local Area Connection and select Properties.
4. In the Local Area Connection Properties dialog box, highlight Internet Protocol Version 4 (TCP/IP), and click the Properties button.
5. The Internet Protocol Version 4 (TCP/IP) Properties dialog box appears. Select the Obtain an IP Address Automatically radio button. If your DHCP server is also configured to assign DNS server addresses, then you can also click the Obtain DNS Server Address Automatically radio button. Then click OK.

If your network adapter is a part of a network bridge, you will not be able to configure TCP/IP properties.

Using APIPA

Automatic Private IP Addressing (APIPA) is used to automatically assign private IP addresses for home or small business networks that contain a single subnet, have no DHCP server, and are not using static IP addressing. If APIPA is being used, then clients will be able to communicate only with other clients on the same subnet that are also using APIPA. The benefit of using APIPA in small networks is that it is less tedious and has less chance of configuration errors than statically assigning IP addresses and configuration.

APIPA is used with Windows Vista under the following conditions:

- The client is configured as a DHCP client, but no DHCP server is available to service the DHCP request.
- The client originally obtained a DHCP lease from a DHCP server, but when the client tried to renew the DHCP lease, the DHCP server was unavailable.

In the next sections you will learn how APIPA works, how to determine if your computer is using APIPA, and how to disable APIPA.

How APIPA Works

By default, a range of Class B network addresses, 169.254.0.1–169.254.255.254, has been set aside as private Class B network addresses. Windows Vista uses this range of addresses to automatically assign IP addresses if APIPA is used.

The steps used by APIPA are as follows:

1. The client will select an address from the range of private Class B addresses that have been allocated, using the subnet mask of 255.255.0.0.
2. The client will use duplicate-address detection to verify that the address that was selected is not already in use.
3. If the address is already in use, the client will repeat steps 1 and 2, for a total of up to 10 retries. If the address is not already in use, the client will configure its interface with the address that was selected.
4. As a background process, the client will continue to search for a DHCP server every five minutes. If a DHCP server replies to the request, the APIPA configuration will be dropped and the client will receive new IP configuration settings from the DHCP server.

Determining if Your Computer Is Using APIPA

To determine if your computer is configured using APIPA, you would use the following command:

```
ipconfig /all
```

The `ipconfig /all` command will produce verbose text. If you see "Autoconfiguration Enabled" within the text and the IP address for your computer is within the 169.254.0.1–169.254.255.254 range, then your computer is using APIPA.

Disabling APIPA

If you want to disable APIPA for a network adapter, you have to configure a statically assigned Alternate Configuration. We will cover how to do that later in this chapter.

Using Static IP Addressing

You can manually configure IP addressing if you know your IP address and subnet mask. If you are using optional components such as a default gateway or a DNS server, you will need to know the IP addresses of the computers that host these services as well. This option is not typically used in large networks because it is time-consuming and prone to user error.

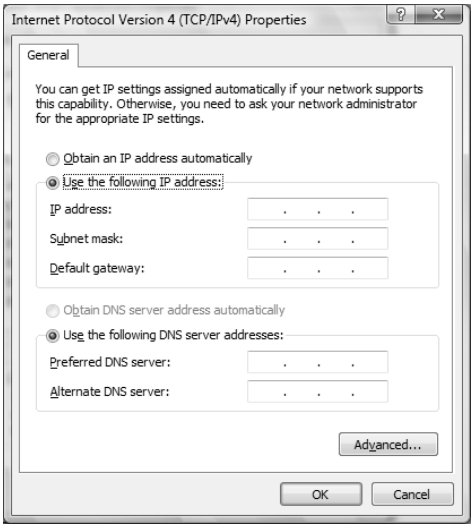
In Exercise 8.3, you will manually configure IP addressing. This exercise assumes that you have a network adapter installed in your computer.

If you are on a "live" network, check with your network administrator before you make any changes to your IP configuration.

EXERCISE 8.3

Manually Configuring IP Addressing

1. Select Start ➢ Network ➢ Network and Sharing Center.
2. In the Network and Sharing Center dialog box, click the Manage Network Connections option. You will see your Local Area Connection as an icon.
3. Right-click Local Area Connection and select Properties.
4. In the Local Area Connection Properties dialog box, highlight Internet Protocol Version 4 (TCP/IP) and click the Properties button.
5. The Internet Protocol Version 4 (TCP/IP) Properties dialog box appears, as shown here. Choose the Use the Following IP Address radio button.



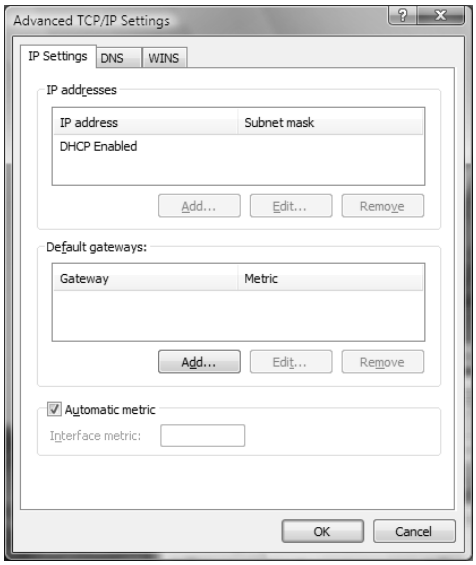
6. In the appropriate text boxes, specify the IP address **131.200.1.1** and subnet mask **255.255.0.0**. Do not specify the default gateway option.
7. Click OK to save your settings and close the dialog box.

Advanced Configuration

Clicking the Advanced button in the Internet Protocol Version 4 (TCP/IP) dialog box opens the Advanced TCP/IP Settings dialog box, shown in Figure 8.37. In this dialog box, you can configure advanced IP, DNS, and WINS settings. The other options that can be configured include the following:

- The IP address that will be used. You can add, edit, or remove IP addresses.
- The default gateways that will be used and the metric associated with each gateway. Metrics are used to calculate the path that should be used through a network.

FIGURE 8.37 The Advanced TCP/IP Settings dialog box



ADVANCED DNS SETTINGS

You can configure additional DNS servers to be used for name resolution and other advanced DNS settings through the DNS tab of the Advanced TCP/IP Settings dialog box, shown in Figure 8.38. The options in this dialog box are described in Table 8.2.

FIGURE 8.38 The DNS tab of the Advanced TCP/IP Settings dialog box

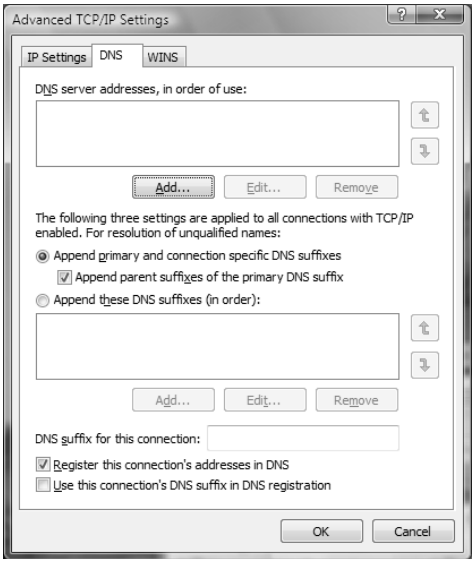


TABLE 8.2 Advanced DNS TCP/IP Settings Options

Option	Description
DNS Server Addresses, in Order of Use	Specifies the DNS servers that are used to resolve DNS queries. Use the arrow buttons on the right side of the list box to move a server up or down in the list.
Append Primary and Connection Specific DNS Suffixes	Specifies how unqualified domain names are resolved by DNS. For example, if your primary DNS suffix is `TestCorp.com` and you type **`ping lala`**, DNS will try to resolve the address as `lala.TestCorp.com`.
Append Parent Suffixes of the Primary DNS Suffix	Specifies whether name resolution includes the parent suffix for the primary domain DNS suffix, up to the second level of the domain name. For example, if your primary DNS suffix is `Nashville.TestCorp.com` and you type **`ping lala`**, DNS will try to resolve the address as `lala.Nashville.TestCorp.com`. If this doesn't work, DNS will try to resolve the address as `lala.TestCorp.com`.
Append These DNS Suffixes (in Order)	Specifies the DNS suffixes that will be used to attempt to resolve unqualified name resolution. For example, if your primary DNS suffix is `TestCorp.com` and you type **`ping lala`**, DNS will try to resolve the address as `lala.TestCorp.com`. If you append the additional DNS suffix `MyCorp.com` and type **`ping lala`**, DNS will try to resolve the address as `lala.TestCorp.com` and `lala.MyCorp.com`.

TABLE 8.2 Advanced DNS TCP/IP Settings Options *(continued)*

Option	Description
DNS Suffix for This Connection	Specifies the DNS suffix for the computer. If this value is configured by a DHCP server and you specify a DNS suffix, it will override the value set by DHCP.
Register This Connection's Addresses in DNS	Specifies that the connection will try to register its addresses dynamically using the computer name that was specified through the System Properties dialog box (accessed through the System icon in Control Panel).
Use This Connection's DNS Suffix in DNS Registration	Specifies that when the computer registers automatically with the DNS server, it should use the combination of the computer name and the DNS suffix.

ADVANCED WINS SETTINGS

You can configure advanced WINS options through the WINS tab of the Advanced TCP/IP Settings dialog box, shown in Figure 8.39. The options in this dialog box are described in Table 8.3.

FIGURE 8.39 The WINS tab of the Advanced TCP/IP Settings dialog box

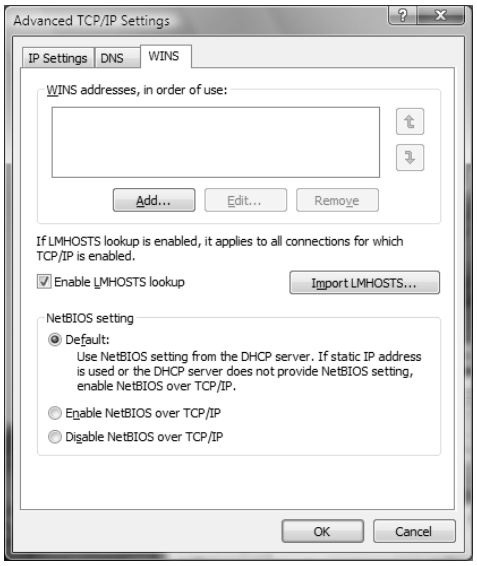


TABLE 8.3 Advanced WINS TCP/IP Settings Options

Option	Description
WINS Addresses, in Order of Use	Specifies the WINS servers that are used to resolve WINS queries. You can use the arrow buttons on the right side of the list box to move a server up or down in the list.
Enable LMHOSTS Lookup	Specifies whether an `LMHOSTS` file can be used for name resolution. If you configure this option, you can use the Import LMHOSTS button to import an `LMHOSTS` file to the computer.
Use NetBIOS Setting from the DHCP Server	Specifies that the computer should obtain its NetBIOS-over-TCP/IP and WINS settings from the DHCP server.
Enable NetBIOS over TCP/IP	Allows you to use statically configured IP addresses so that the computer is able to communicate with pre–Windows XP computers (NetBIOS was discontinued with XP).
Disable NetBIOS over TCP/IP	Allows you to disable NetBIOS over TCP/IP. Use this option only if your network includes only Windows XP clients, Windows Vista clients, or DNS-enabled clients.

Using Multiple IP Addresses

Windows Vista allows you to configure more than one network adapter in a single computer, which is referred to as *multihoming*. Windows Vista also supports logical multihoming, which is when multiple IP addresses are configured for a single network adapter. You would use logical multihoming if you had a single physical network that was logically divided into subnets and you wanted your computer to be associated with more than one subnet.

To configure multiple IP addresses for a single network adapter, you would take the following steps:

1. Select Start ➢ Network ➢ Network and Sharing Center ➢ Manage Network Connections.
2. Right-click the Local Area Connection icon and click Properties.
3. In the Local Area Connection Properties dialog box, highlight Internet Protocol Version 4 (TCP/IP), and click the Properties button.
4. In the Internet Protocol Version 4 (TCP/IP) Properties dialog box, verify that Use the Following IP Address is selected and configured with IP address information.
5. From the Internet Protocol Version 4 (TCP/IP) Properties dialog box, click the Advanced button to access the Advanced TCP/IP Settings dialog box. On the IP Settings tab (shown in Figure 8.37), under IP Addresses, click the Add button. You will then be able to assign

additional IP addresses and subnet mask settings. Click Add after you have entered an IP address and subnet mask. Repeat this step to add any additional IP addresses.

6. If you need to assign more than one default gateway to your IP configuration, use the Default Gateways section of Advanced IP Settings.

Using Alternate Configuration

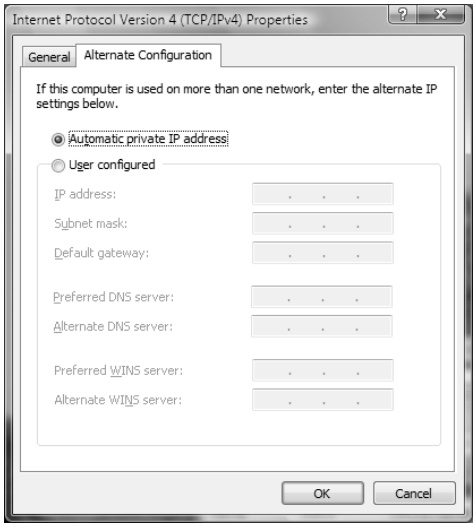
Alternate Configuration is designed to be used by laptops and other mobile computers to manage IP configurations when the computer is used in multiple locations and one location requires a static IP address and the other location(s) require dynamic IP addressing. For example, a user with a laptop might need a static IP address to connect to their broadband ISP at home, and then use DHCP when connected to the corporate network.

Alternate Configuration works by allowing the user to configure the computer so that it will initially try to connect to a network using DHCP; if the DHCP attempt fails (for example, when the user is at home), the alternate static IP configuration is used. The alternate IP address can be an Automatic Private IP Address (APIPA) or a manually configured IP address.

To configure Alternate Configuration, you would take the following steps:

1. Click Start ➢ Network ➢ Network and Sharing Center ➢ Manage Network Connections.
2. Right-click the Local Area Connection icon and click Properties.
3. In the Local Area Connection Properties dialog box, highlight Internet Protocol Version 4 (TCP/IP), and click the Properties button.

FIGURE 8.40 The Alternate Configuration tab of the Internet Protocol Version 4 (TCP/IP) Properties dialog box



4. The Internet Protocol Version 4 (TCP/IP) Properties dialog box appears. On the General tab, verify that the Obtain an IP Address Automatically radio button is selected. Click the Alternate Configuration tab, as shown in Figure 8.40.
5. If you want to use APIPA to assign the alternate address, select the Automatic Private IP Address option. If you want to disable APIPA, you must manually configure a static address by selecting the User Configured option. You would then need to supply the IP address, subnet mask—and, if needed, default gateway, preferred and alternate DNS servers, and preferred and alternate WINS servers. Then click OK.

Using IPv6 Addresses

Windows Vista natively supports IP version 4 (IPv4) and IP version 6 (IPv6). The primary differences between IPv4 and IPv6 is that IPv6 has improvements over IPv4, including more simplified support for installation and configuration of wireless devices and more support for smart network–enabled devices. IPv6 is designed to coexist with IPv4, and most of the Internet traffic generated by IPv6 actually tunnels over existing IPv4 Internet infrastructure.

One of the drawbacks to IPv4 is the lack of available address space. IPv4 uses 32-bit addresses, which allows for only 4,294,967,296 unique addresses, some of which are used for private networks, diagnostics, and multicasting. IPv6 alleviates the address space shortage by using 128-bit addresses, which could allow 7 billion people to each have 4.8×10^{28} unique addresses.

IPv6 addresses are typically written as eight groups of four hexadecimal characters. Each group of characters is separated by a colon. An example of a valid IPv6 address is 0123:0456:0789:0000:0000:00AB:00CD:00EF.

Leading zeroes can be omitted, so we can write our example address as 123:456:789:0:0:AB:CD:EF. Additionally, a double colon can be used to compress a set of consecutive zeroes, so we can write our example address as 123:456:789::AB:CD:EF.

You cannot write an IPv6 address with two double-colons; only one double-colon can be used to compress one set of consecutive zeroes.

Even with IPv4's lack of address space, we will probably continue to use IPv4 for many years, running IPv6 alongside IPv4. Many mechanisms exist for enabling IPv6 communications over an IPv4 network, including the following:

- Dual Stack - a computer that runs both the IPv4 and IPv6 protocol stacks
- 6to4 and Toredo Tunneling - encapsulating IPv6 traffic inside an IPv4 packet

Some IPv6-to-IPv4 dynamic translation techniques require that a computer's IPv4 address is used as the last 32 bits of the IPv6 address. When these translation techniques are used, it is common to write the last 32 bits as you would typically write an IPv4 address, such as 1234:5678:90AB:CDEF:1234:5678:192.168.122.26.

Additional TCP/IP Features and Options

TCP/IP is complex and offers many features. In addition to having a basic understanding of TCP/IP and being able to configure and manage basic IP configurations on a Windows Vista computer, you should be aware of some other key features and options of TCP/IP. The TCP/IP features and options that will be covered in greater detail in the following subsections include:

- Understanding TCP/IP name resolution
- Using multiple IP addresses
- Testing and verifying TCP/IP connectivity

Understanding TCP/IP Name Resolution

When users try to access a network resource, it is unusual for them to access the resource via an IP address. In Windows environments, users typically access resources using a hostname or a NetBIOS name. The methods used to manage TCP/IP name resolution are:

- DNS
- NetBIOS over TCP/IP (NetBT)
- WINS
- HOSTS or LMHOSTS files
- Subnet broadcasts

Domain Name System (DNS) is a global, distributed database that is based on a hierarchical naming system. DNS name resolution is used to name DNS-based names (friendly usernames such as `BrainBeacon.com`) to IP addresses. Windows 2000 and Windows 2003 domains inherently use DNS services, and DNS is the default name resolution method used.

Microsoft clients that are using Windows *9x*, Windows Me, or other early implementations of Windows operating systems rely on NetBIOS names to identify computers on the network. Windows 2000 Server and Windows Server 2003 use a service called Windows Internet Name Service (WINS) for compatibility with applications and services that use NetBIOS services to map the NetBIOS name to an IP address.

`HOSTS` and `LMHOSTS` files are local files that provide hostname-to-IP address resolution. However, these files must be maintained manually. This is not a common method of resolving IP addresses, as it is administrator intensive and prone to configuration errors.

If no name resolution method is configured for NetBIOS, the final way that address resolution is attempted is through the use of subnet broadcasts. You typically want to avoid these broadcasts since they are directed to all computers on the subnet as opposed to being sent only to the specified computer as a unicast transmission.

Testing IP Configuration

After you have installed and configured the TCP/IP settings, you can test the IP configuration using the `ipconfig`, `ping`, and `nbtstat` commands. These commands are also very useful in troubleshooting IP configuration errors. You can also graphically view connection details through Local Area Connection Status. Each command is covered in detail in the following subsections.

The *ipconfig* Command

The *ipconfig* command displays your IP configuration. Table 8.4 lists the command switches that can be used with the `ipconfig` command.

TABLE 8.4 *ipconfig* Switches

Switch	Description
`/?`	Shows all of the help options for `ipconfig`
`/all`	Shows verbose information about your IP configuration, including your computer's physical address, the DNS server you are using, and whether you are using DHCP
`/allcompartments`	Shows IP information for all compartments
`/release`	Releases an IPv4 address that has been assigned through DHCP
`/release6`	Releases an IPv6 address that has been assigned through DHCP
`/renew`	Renews an IPv4 address through DHCP
`/renew6`	Renews an IPv6 address through DHCP
`/flushdns`	Purges the DNS Resolver cache
`/registerdns`	Refreshes DHCP leases and re-registers DNS names
`/displaydns`	Displays the contents of the DNS Resolver Cache
`/showclassid`	Lists the DHCP class IDs allowed by the computer
`/setclassID`	Allows you to modify the DHCP class ID

In Exercise 8.4, you will verify your configuration with the `ipconfig` command. This exercise assumes that you have a network adapter installed in your computer and have completed Exercise 8.3.

EXERCISE 8.4

Using the *ipconfig* Command

1. Select Start ➢ All Programs ➢ Accessories ➢ Command Prompt.
2. In the Command Prompt dialog box, type **`ipconfig`** and press Enter. Note the IPv4 address, which should be the address that you configured in Exercise 8.3.
3. In the Command Prompt dialog box, type **`ipconfig /all`** and press Enter. You now see more information. Close the command prompt window when you have finished viewing the information.

The *ping* Command

The *ping* command is useful for verifying connectivity between two hosts. The command sends an ICMP (Internet Control Message Protocol) Echo Request to a remote computer, and receives an ICMP Echo Reply if the remote computer is available.

You can ping a computer based on the computer's IP address or the DNS name. If you were using an IP address, the `ping` command would have the following syntax:

```
ping IPaddress
```

For example, if you want to verify whether the computer with IP address 131.200.2.30 is available on the network, you would type the following command:

```
ping 131.200.2.30
```

If you were using a DNS name, the `ping` command would have the following syntax:

```
ping DNSname
```

For example, if you want to verify whether a computer with the DNS name `Example.BrainBeacon.com` is available on the network, you would type the following command:

```
ping Example.BrainBeacon.com
```

If you were having trouble connecting to a host on another network, `ping` would help you verify that a valid communication path existed. You might `ping` the following addresses:

- The loopback address, 127.0.0.1
- The local computer's IP address (you can verify this with `ipconfig`)

- The local router's (default gateway's) IP address
- The remote router's IP address
- The remote computer's IP address

If `ping` failed to get a reply from any of these addresses, you would have a starting point for troubleshooting the connection error. The error messages that can be returned from a `ping` request include the following:

- TTL Expired in Transit, which means that the packet exceeded the number of hops specified to reach the destination host computer. Each time a packet passes through a router, the Time To Live (TTL) counter reflects the pass through the router as a hop. You can use the `ping -i` parameter to increase TTL. This error can also be due to a routing configuration error, which has resulted in a routing loop. The `tracert` command can be used to identify routing loops.
- Destination Host Unreachable, which is generated when a local or remote route path does not exist between the sending host and the specified destination computer. This error could occur because the router is misconfigured or the target computer is not available.
- Request Timed Out, which means that the Echo Reply message was not received from the destination computer within the time allotted. By default, destination computers have four seconds to respond. You can change the timeout value with the `ping -w` parameter.
- Ping Request Could Not Find Host, which indicates that the destination hostname couldn't be resolved. Verify that the destination hostname was properly specified, that all DNS and WINS settings are correct, and that the DNS and WINS servers are available.

The *nbtstat* Command

NBT is NetBIOS over TCP/IP, and the `nbtstat` command is used to display TCP/IP connection protocol statistics over NBT. Table 8.5 lists the command-line options that can be used.

TABLE 8.5 *nbtstat* Command-Line Options

Switch	Option	Description
`/?`	Help	Shows all of the help options for `nbtstat`
`-a`	Adapter Status	Shows adapter status and lists the remote computer's name, based on the hostname you specify
`-A`	Adapter Status	Shows adapter status and lists the remote computer's name, based on the IP address you specify
`-c`	Cache	Displays the NBT cache of remote computers through their names and IP addresses
`-n`	Names	Shows a list of the local computer's NetBIOS names

TABLE 8.5 *nbtstat* Command-Line Options *(continued)*

Switch	Option	Description
-r	Resolved	Shows a list of computer names that have been resolved either through broadcast or WINS
-R	Reload	Causes the NBT remote cache name table to be purged and reloaded (must be logged on as an administrator with privilege elevation)
-S	Sessions	Shows the current sessions table with the destination IP addresses
-s	Sessions	Shows the current sessions table and the converted destination IP address to the computer's NetBIOS name
-RR	Release Refresh	Sends a Name Release packet to the WINS server and then starts a refresh

TCP/IP Troubleshooting

If you are having trouble connecting to network resources, you might want to check the following:

- Use IPConfig to ensure that you are not configured with an APIPA address. If so, determine why you are not receiving IP settings from your DHCP server.
- If you can access a resource (for example, by pinging a computer) by IP address, but not by name, you should check the DNS settings on your computer.
- If you can access resources on your local subnet but not on a remote subnet, you should check the default gateway settings on your computer.
- If you can access some but not all resources on your local subnet or remote subnet, you should check your subnet mask settings, the wiring to those resources, or the devices between your computer and those resources.

Summary

This chapter described how to configure network connections. We covered the following topics:

- Installing, configuring, and troubleshooting network adapters. You configure a network adapter through its Properties dialog box.
- Using the Network and Sharing Center to configure network connections.
- Configuring a computer for remote access connectivity.

- Remote security and the authentication methods and remote data encryption options that are used with Windows Vista.
- Configuring a wireless network.
- Installing, configuring, and testing network protocols.

Exam Essentials

Be able to install, configure, and troubleshoot network adapters. Know how to configure network adapters. Be familiar with troubleshooting network adapter problems that keep a client from attaching to the network.

Be familiar with the Network and Sharing Center. Know how to use the Network and Sharing Center to configure networks, network locations, sharing and discovery, and network connections.

Be able to configure a remote access connection. Know how to configure RAS and VPN connections. Become familiar with the different authentication and encryption options.

Be able to connect to and troubleshoot network devices. Know how to automatically and manually connect to network projectors and printers.

Be able to create and troubleshoot a wireless network. Know how to configure wireless network adapters. Know how to roll out wireless network configurations to multiple computers. Know how to troubleshoot network adapter problems that keep a client from attaching to a wireless network.

Be able to configure and troubleshoot TCP/IP. Know the primary purpose and configuration options for TCP/IP, DHCP, WINS, and DNS. Know how to troubleshoot protocol-related network problems. Know how to use `ipconfig`, `ping`, and `nbtstat`.

Review Questions

1. You are configuring a new wireless network for a group of Windows XP and Windows Vista computers. After configuring the wireless network, you save the configuration to a USB key. Which file on the USB key is used to launch the Wireless Network Setup Wizard?

   A. `setupSNK.exe`

   B. `SNKsetup.exe`

   C. `SETTING.wfc`

   D. `WSETTING.exe`

2. You are a salesperson who travels from city to city, giving sales presentations to prospective clients. When not traveling, you work from home on your secure network. What network location profile should you use while working from home?

   A. Domain

   B. Home

   C. Public

   D. Private

3. You are responsible for giving a presentation at a convention. The convention center has provided you with a wireless network projector and has supplied you with the information to connect to the wireless network. After you configure your computer to connect to the wireless network, what would you use to connect to the wireless network projector?

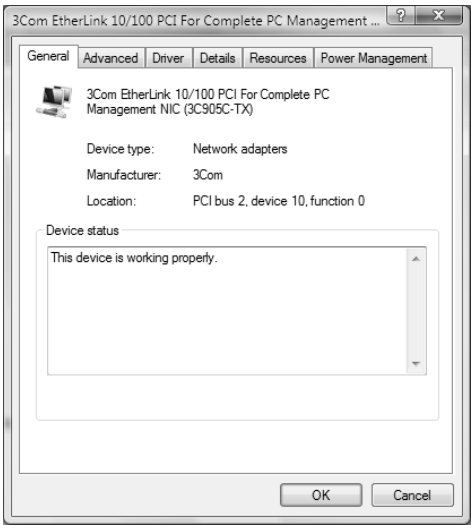
   A. Network and Sharing Center

   B. Connect to a Network Projector

   C. Wireless Network Setup Wizard

   D. Sharing and Discovery

4. You have a network adapter that is not able to correctly attach to the network. You discover that the driver you are using is outdated and there is an updated driver that will likely solve your problem. In the network adapter's Properties dialog box, shown here, what tab should you select?



   A. Advanced
   B. Driver
   C. Details
   D. Resources

5. Your computer is called WS1. You are not able to access any network resources. You know that WS2 can access the network, and you want to test communication between WS1 and WS2. Which command would you use to test communications with another computer based on its IP address?

   A. `ipconfig`
   B. `testip`
   C. `ping`
   D. `finger`

6. You use your Windows Vista laptop to access the Internet wirelessly from many locations. As a result, you have configured the settings for many different wireless networks on your laptop. If multiple wireless connections are available, to which wireless network will your laptop connect?

   A. Your laptop will connect to the wireless connection that is listed highest in the Manage Wireless Networks list.

   B. Your laptop will connect to the wireless connection that is listed first alphabetically.

   C. Your laptop will connect to the closest wireless connection.

   D. Your laptop will connect to the wireless connection with the strongest signal.

7. You configure a Windows Vista computer and connect it to your network. The network contains many computers in a workgroup configuration. You enable File Sharing and configure your computer so that the default shared folders are available. Which folders will be available to users in the workgroup?

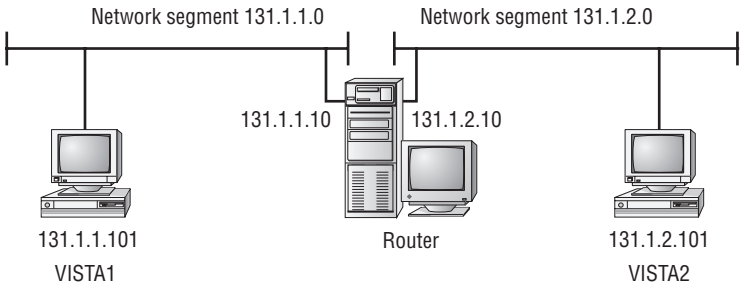
   A. Public

   B. Printers

   C. Users

   D. Windows

8. Suzanne is sitting at computer VISTA1. She wants to be able to access resources on VISTA2. Based on the following diagram, how should Suzanne configure her default gateway?



   A. 131.1.1.0

   B. 131.1.1.10

   C. 131.1.2.0

   D. 131.1.2.10

9. You are the network administrator for a small company. External access to the network is available by VPN. You need to connect to your company's network from home using your Windows Vista computer. Which tunneling protocols are available to you by default?

   A. GTP

   B. L2TP

   C. PPTP

   D. Teredo

10. When you try to access the `sales.acmecorp.com` server, you can access the server using the server's IP address but not the fully qualified domain name. Which configuration file can you use to alleviate this problem?

    A. HOSTS

    B. LMHOSTS

    C. `dns.txt`

    D. `wins.txt`

11. You connect a new Windows Vista computer to your network. Afterwards, you attempt to browse to web pages on the Internet, but are unable to do so. You can ping other computers on your network but cannot ping servers on the Internet. What network icon should you expect to see in the lower-right corner of the taskbar?

    A. Two computers

    B. Two computers with a globe

    C. Two computers with a red X

    D. Two computers with a yellow exclamation point

12. You purchase an 802.11g wireless network card for your Windows Vista computer so that you can connect it to the wireless network at your company. The wireless access point uses the 802.11a standard using WPA encryption, and SSID broadcasts are enabled. When you attempt to connect to the network, the SSID is not displayed in the list of wireless networks. What is the most likely problem?

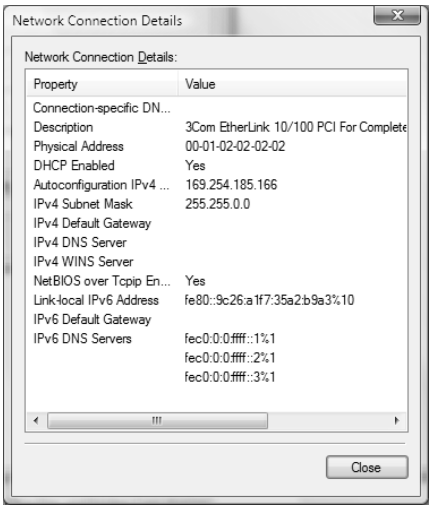
    A. Your computer is configured with the wrong SSID.

    B. MAC address filtering is enabled on the wireless access point.

    C. The wireless network card is not compatible with the wireless access point.

    D. Windows Vista does not support WPA encryption.

13. You configure a new Windows Vista computer on your company's network. After you boot the computer, you do not have any access to network resources. When you view the connection status details, you see the following dialog box:



What is the most likely problem?

A. The computer is configured with the wrong static IP address.

B. The computer is configured with the wrong subnet mask.

C. The computer cannot access the DNS server.

D. The computer cannot access the DHCP server.

14. You have two DHCP servers on your network. Your computer accidentally received the wrong IP and DNS server configuration from a DHCP server that was misconfigured. The DHCP server with the incorrect configuration has been disabled. What command would you use to release and renew your computer's DHCP configuration?

A. `ipconfig`

B. `dhcprecon`

C. `release`

D. `ipadjust`

15. You are the network administrator for your company. Your service provider has assigned you the network address 200.200.200.0. You have been granted the entire range to use. What class of address have you been assigned?

A. Class A

B. Class B

C. Class C

D. Class D

16. You are the network administrator for your company. After configuring a new computer and connecting it to the network, you discover that you cannot access any of the computers on the remote subnet by IP address. You can access some of the computers on the local subnet by IP address. What is the most likely problem?

    A. Incorrectly defined IP address

    B. Incorrectly defined subnet mask

    C. Incorrectly defined default gateway

    D. Incorrectly defined DNS server

17. A user tells you that they cannot access a server in the domain. After troubleshooting, you determine that the user cannot access the server by name but can access the server by IP address. What is the most likely problem?

    A. Incorrectly defined IP address

    B. Incorrectly defined subnet mask

    C. Incorrectly defined DHCP server

    D. Incorrectly defined DNS server

18. You are attempting to configure a new laptop to connect to a wireless network. When you scan for available networks, you see the entry "Unnamed Network." What is the first thing you will need in order to connect to the wireless network?

    A. The SSID

    B. The WPA key

    C. The MAC address of your laptop's wireless NIC

    D. The wireless standard used

19. You are the network administrator for a small electronics company. The computers on your network are configured with the HOSTS files. After making a change to the HOSTS file on a computer on your network, what command must you run if you do not want to reboot the computer?

    A. `netstat -r`

    B. `netstat -R`

    C. `nbtstat -r`

    D. `nbtstat -R`

20. You are configuring your Windows Vista computer to connect to your company network over VPN. You want to connect securely, so you do not want to send your password using clear text. Which authentication method do you want to avoid?

    A. CHAP

    B. EAP

    C. MS-CHAPv2

    D. PAP

Answers to Review Questions

1. A. The `setupSNK.exe` file launches the Wireless Network Setup Wizard. This file can be used to easily import wireless network configurations into computers running Windows XP with Service Pack 2 and Windows Vista.

2. D. You should use the Private network location profile when at home. The Private network location profile indicates that you are on a secure, private network. The Private network location allows your computer to discover and connect to other computers and devices, and allows your computer to be discovered by other devices.

3. B. You should use the Connect to a Network Projector application to connect to the wireless network projector. To connect, you can either search for the projector or you can enter the IP address or name of the projector. You will also need the password if the projector is configured with one.

4. B. You use the settings in the Driver tab to uninstall or update a device driver. If the new driver does not work, you can use the Roll Back Driver option to return to the previous driver that was working.

5. C. The `ping` command is used to send ICMP Echo Request and Echo Reply messages between two IP hosts to test whether a valid communication path exits. If no valid path exists, the `tracert` command can be used to trace where in the communications path the error exists.

6. A. Your laptop will connect to the wireless connection that is listed highest in the Manage Wireless Networks list. Wireless networks listed higher on the list have a higher priority. You can adjust the priority of each network by moving it up or down on the list.

7. A, B, C. The Public, Printers, and Users folders will be available to users in the workgroup. The Windows folder will not be available.

8. B. Suzanne needs to configure the default gateway with the IP address of the router connection that is attached to her subnet, 131.1.1.10. If her default gateway is not properly configured, she will be able to communicate only with other computers on her subnet.

9. B, C. Windows Vista supports using Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) by default. You should configure your Windows Vista computer to use the tunneling protocol that you have configured on your VPN device at your company. The GPRS Tunneling Protocol (GTP) and Teredo are not included with Windows Vista.

10. A. If you do not have access to a properly configured DNS server, you can use a HOSTS file to map IP addresses to domain hostnames. This option is not commonly used in large networks, as it is administrator intensive and is prone to user errors.

11. A. You should expect to see an icon with two computers. This means that you have local connectivity, but you do not have Internet connectivity. You would see two computers with a globe if you were connected to the Internet, and you would see two computers with a red X if you did not have any network connectivity at all. You would not ever see two computers with a yellow exclamation point.

12. C. The wireless network card, which uses 802.11g, is not compatible with the wireless access point, which uses 802.11a. The 802.11g standard is backward compatible with 802.11b, and uses the same frequency range. However, the 802.11a standard uses a different frequency range.

13. D. Your computer has received an APIPA address. This usually occurs because the computer is configured to receive IP address information from a DHCP server, and the computer cannot access the DHCP server.

14. A. You can release your DHCP configuration with the `ipconfig /release` command, and renew your DHCP configuration with the `ipconfig /renew` command. Then your IP address and DNS server address will be provided by the correct DHCP server.

15. C. You have been assigned a Class C address. Class C addresses have a first octet from 192 through 223.

16. B. The new computer probably has an incorrectly defined subnet mask. Subnet masks are used to specify which part of the address is the network address and which part of the address is the host or client address. An improperly configured subnet mask can cause some or all of the computers on local or remote networks to be inaccessible.

17. D. The user's computer cannot access the server by name because it probably has an incorrectly defined DNS server. DNS servers are used to resolve domain names to IP addresses.

18. A. The first thing you will need is the name of the wireless network, or SSID. An SSID that is hidden can be displayed as "Unnamed Network." After you have specified the SSID, the wireless network may require a key or a passphrase.

19. D. You must run the `nbtstat -R` command to clear and reload the NetBIOS cache. This should be done after making changes to the LMHOSTS or HOSTS files. Rebooting the computer will also clear and reload the cache.

20. D. If you want to connect securely, you want to avoid using Password Authentication Protocol (PAP). PAP sends passwords in clear text format. Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), and Extensible Authentication Protocol (EAP) all use encrypted passwords.

Chapter

9

Configuring Internet Explorer

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring and Troubleshooting Post-Installation Settings**
  - Configure Windows Internet Explorer
- ✓ **Configuring Windows Security Features**
  - Configure Dynamic Security for Internet Explorer 7

Windows Vista ships with Internet Explorer 7 (IE) to access Internet and intranet resources. This latest release of Internet Explorer has been greatly enhanced to provide increased security and usability. Usability enhancements include tabbed browsing, support for RSS, and the ability to add numerous add-ons to enhance your browsing experience. Security enhancements include antiphishing filters, parental controls, pop-up blockers, and increased privacy control.

In this chapter, you will learn about the new features of IE. Additionally, you will learn how to configure basic and advanced configuration options for IE to improve both security and usability.

Overview of Internet Explorer

Internet Explorer (IE) is a web browser used to search and view information on the World Wide Web (WWW) via the Internet or information that is stored on local intranets. You can access resources by typing in the address of the web page you wish to access or by selecting an address from your Favorites list. In this section you will learn about accessing resources through IE.

Accessing Resources through Internet Explorer

When you access a resource through IE, you use a Uniform Resource Locator (URL) address. A URL address is typically composed of four parts—for example, `http://www.sybex.com`.

- The first part of the address is the protocol that is being used. Examples of protocols include HTTP and FTP.
- The second part of the address is the location of the site—for example, the World Wide Web (`www`).
- The third part of the address is who maintains the site—for example, Sybex.
- The fourth part of the address identifies the kind of organization. Examples of defined suffixes include `.com`, `.gov`, `.org`, and `.edu`.

Using HTTP

HTTP is the main protocol for making web requests. HTTP defines how messages are formatted and transmitted and the actions that will be executed by web servers and browsers based

on the requests you make. The main standard that is used with HTTP is Hypertext Markup Language (HTML), which defines how web pages are formatted and displayed.

If the web server you are trying to access is using Secure Sockets Layer (SSL) services, then instead of using http:// requests, you would use secure HTTP, and the request would use https://.

Using FTP

FTP is mainly used to transfer files between computers on the Internet. Access to FTP servers is based on permissions that have been set on the FTP server you are trying to access. Access can be granted to anonymous users, or users can be required to have a valid username and password.

Once you access an FTP site, you can

- Work with files and folders in the same manner that would be used on a local computer
- View, download, upload, rename, and delete files and folders (based on your permissions)

When you use FTP for file transfer with IE, the syntax looks different than a typical HTTP request. FTP requests are made through the address bar on IE. For example, if you were trying to access Microsoft's FTP site, you would type

```
ftp://ftp.microsoft.com
```

If you need to provide logon credentials as a part of the FTP request, then the syntax you would use would be

```
ftp://username:password@ftp.microsoft.com
```

Usability Features of Internet Explorer 7

Internet Explorer 7 contains many usability improvements over previous versions of IE. The following list indicates the new usability improvements in IE:

- Reorganized user interface to reduce clutter and to maximize the web page viewing area
- An Instant Search box to enable you to search the Web from the IE toolbar without having to install other third-party search toolbars
- Automatic Really Simple Syndication (RSS) detection and support
- Tabbed browsing support, which allows you to view multiple websites in a single browser window
- Pop-up Blocker, which blocks websites from displaying pop-up windows

- Add-on support that enables you to increase the functionality of IE by installing add-ons created by Microsoft as well as by third parties
- A Favorites Center that provides quick access to bookmarked links and RSS subscriptions

In the following sections, you will learn more about configuring usability options in IE.

Configuring Instant Search

The Instant Search box in IE provides quick access to Internet search capabilities without the need to load a new web page or to install third-party toolbars. The Instant Search box is located in the upper-right corner of the IE user interface, as shown in Figure 9.1.

By default, the Instant Search box is configured to use Microsoft's Windows Live search provider to search the Internet. However, other search providers can be added to the Instant Search box, such as Amazon.com and Microsoft.com, or you can create your own search provider. You can configure new search providers by clicking the arrow next to the Instant Search box and selecting Find More Providers, which will open the Add Search Providers to Internet Explorer 7 web page, as shown in Figure 9.2.

Selecting a search provider on the Add Search Providers to Internet Explorer 7 web page will open the Add Search Provider dialog box, as shown in Figure 9.3. When adding new search providers to IE, you can configure the new provider as the default search provider by selecting the Make This My Default Search Provider check box.

Once you have configured new search providers in IE, you can change the Instant Search box default search provider by clicking the arrow next to the Instant Search box and selecting Change Search Defaults, which opens the Change Search Defaults dialog box. Figure 9.4 displays this dialog box.

In Exercise 9.1, you will install and configure the Amazon.com search provider as the default search provider for IE.

EXERCISE 9.1

Configuring Amazon.com as the Default Search Provider for Instant Search

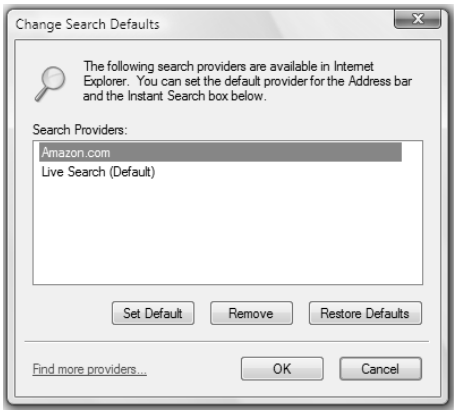
1. Select Start ➢ Internet to open Internet Explorer.
2. Click the arrow next to the Instant Search box, and select Find More Providers.
3. On the Add Search Providers to Internet Explorer web page, select Amazon under Topic Search.
4. Select the Make This My Default Search Provider option in the Add Search Provider dialog box and click Add Provider. The Amazon.com search provider will become the default search provider for Instant Search.

FIGURE 9.1 The Instant Search box

FIGURE 9.2 The Add Search Providers to Internet Explorer 7 web page

FIGURE 9.3 The Add Search Provider dialog box

FIGURE 9.4 The Change Search Defaults dialog box



Configuring RSS

RSS is a content syndication technology that enables a website to syndicate content via an RSS file, which is a formatted XML document. Visitors to the site can subscribe to the RSS feed, and any updates to the website will be automatically downloaded locally to the visitor's computer and will be readable by any RSS-capable application without the need for the visitor to revisit the website.

Microsoft has added RSS support across many of its websites to enable you to easily and automatically receive updates and information about Microsoft products whenever new information is published. For example, on Microsoft's TechNet and MSDN sites, you can subscribe to RSS feeds to obtain the latest news and articles as soon as they are published. Furthermore, Microsoft has added the ability to subscribe to search results so that you can be updated when

new information that matches a search result is published. Figure 9.5 displays a list of search results for Internet Explorer on Microsoft's TechNet website. At the top of the search results, you are given the option of subscribing to the results of the search.

IE 7 adds support for automatically detecting and reading RSS feeds found on web pages. When you open a web page in IE that contains an RSS feed, an orange RSS icon located on the toolbar is highlighted to indicate that an RSS feed is available. For web pages that do not contain RSS feeds, the RSS icon is grayed out. When the RSS icon is highlighted, you can click the

FIGURE 9.5 Subscribing to search results

icon to view the RSS feed using IE's RSS reading functionality. If you are not subscribed to a feed, you have the option of subscribing to the feed when viewing it, as shown in Figure 9.6.

If the Turn On Feed Reading View option of the Feed Settings dialog box is disabled, then clicking the RSS icon in Internet Explorer will display the XML of the underlying RSS feed instead of utilizing the feed reader in IE. The Turn On Feed Reading View option is enabled by default.

Clicking Subscribe to this feed opens the Subscribe to This Feed dialog box, where you can select where to store the subscription in the Favorites Center. The Subscribe to This Feed dialog box is shown in Figure 9.7.

You can view the feeds to which you are subscribed by opening the Favorites Center by clicking Alt+C or by clicking the star icon on the IE toolbar. The Feeds section of the Favorites Center is shown in Figure 9.8.

FIGURE 9.6 Viewing an RSS feed in IE

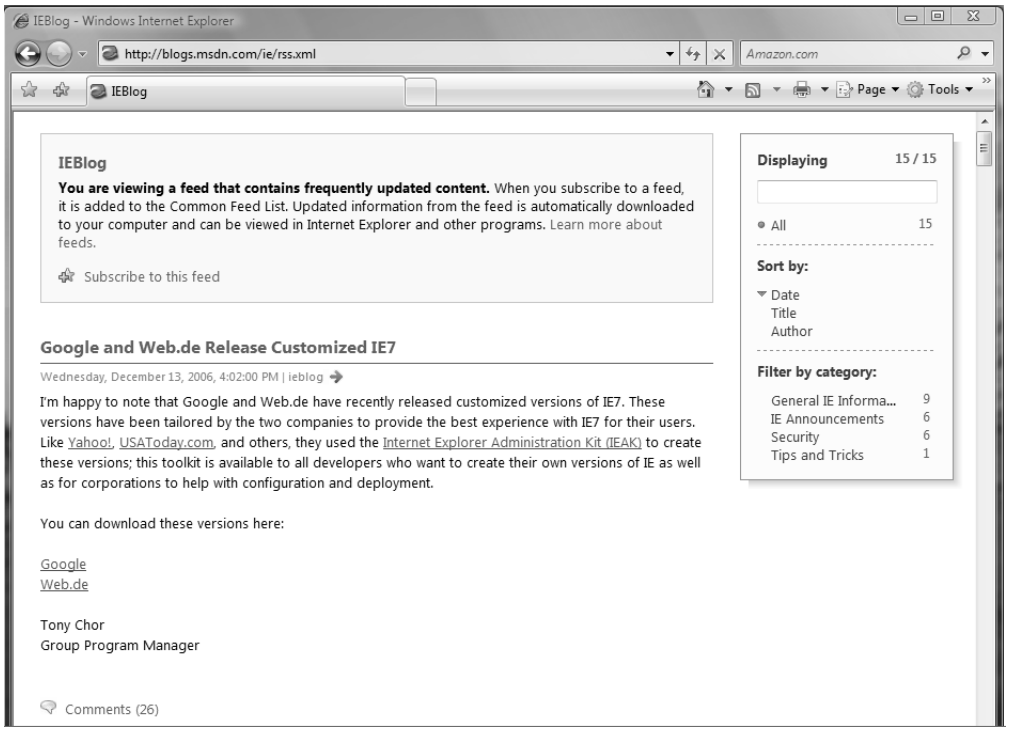
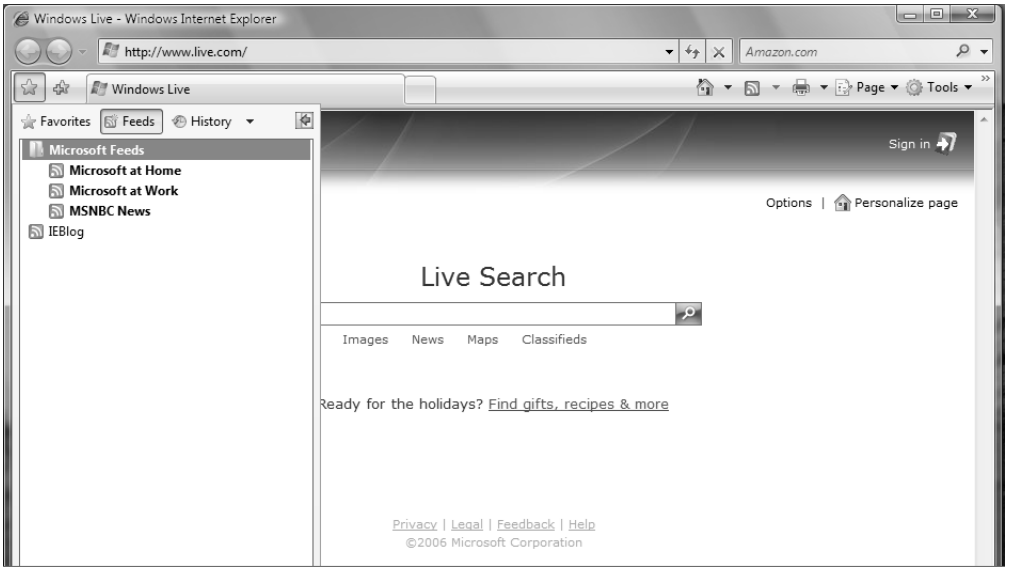


FIGURE 9.7 The Subscribe to This Feed dialog box

FIGURE 9.8 RSS Feeds in the Favorites Center



Configuring RSS Feed Properties

After subscribing to a website's RSS feed, you can configure several options for that feed, such as how often the RSS feed is checked for updates, whether attachments included in that feed should automatically be downloaded, and how many updates should be saved. To modify the properties of an RSS feed, you should open the Feed Properties dialog box by opening Internet Explorer, clicking the star icon, selecting Feeds, clicking the RSS feed to modify, and clicking View Feed Properties. The Feed Properties dialog box is shown in Figure 9.9.

FIGURE 9.9 The Feed Properties dialog box

If you subscribe to an RSS feed that often contains attachments such as audio or video files, you should configure the attachments to be downloaded automatically.

In Exercise 9.2, you will configure feed properties for an RSS feed.

EXERCISE 9.2

Configuring RSS Feed Properties

1. Select Start ➢ Internet to open Internet Explorer.
2. Select the Star icon to open Favorites Center, and click Feeds.
3. Right-click a feed in the Feeds list, and select Properties.
4. Click the Settings button, and configure the Automatically Check Feeds for Updates drop-down list to 4 hours in the Feed Settings dialog box. Click OK.
5. Select the Automatically Download Attached Files check box.
6. Click OK.

Configuring Add-ons

IE provides the ability to install add-ons to extend the functionality of the browser. Add-ons can be used to improve usability and security, or simply to provide entertainment. Add-ons are created not only by Microsoft but by third parties as well.

To install, enable or disable add-ons, you should expand the Tools toolbar option in IE and select Manage Add-ons, as shown in Figure 9.10.

The Manage Add-ons menu contains two submenu items: Enable or Disable Add-ons and Find More Add-ons. Add-ons can be installed by clicking Find More Add-ons and selecting the desired add-on from the list displayed on the Add-ons for Internet Explorer web page. The add-on will be downloaded and you can then install the add-on. Once installed, you can enable or disable the add-on by accessing the Manage Add-ons menu and clicking Enable or Disable Add-ons, which will open the Manage Add-ons dialog box. Any add-ons that are currently loaded in IE will be displayed in the Manage Add-ons dialog box, as shown in Figure 9.11.

The Show list of the Manage Add-ons dialog box provides several options for viewing and managing add-ons installed in IE. Table 9.1 describes the options provided by the Show list.

FIGURE 9.10 The Manage Add-ons option of the Tools menu

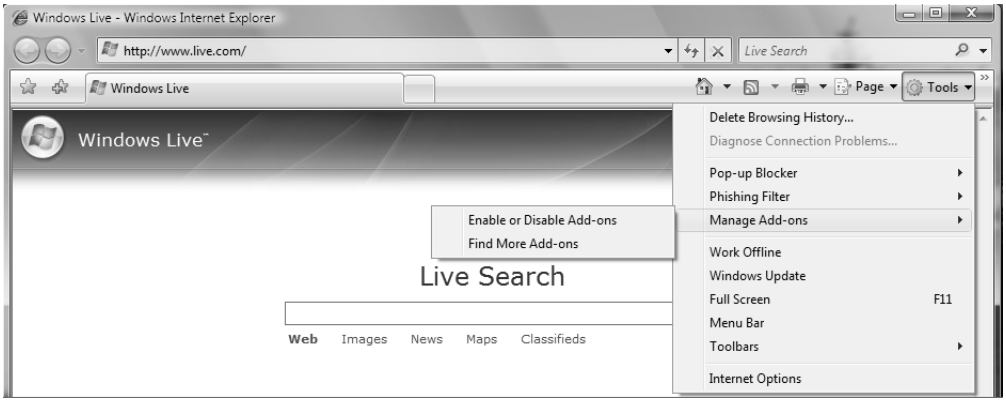


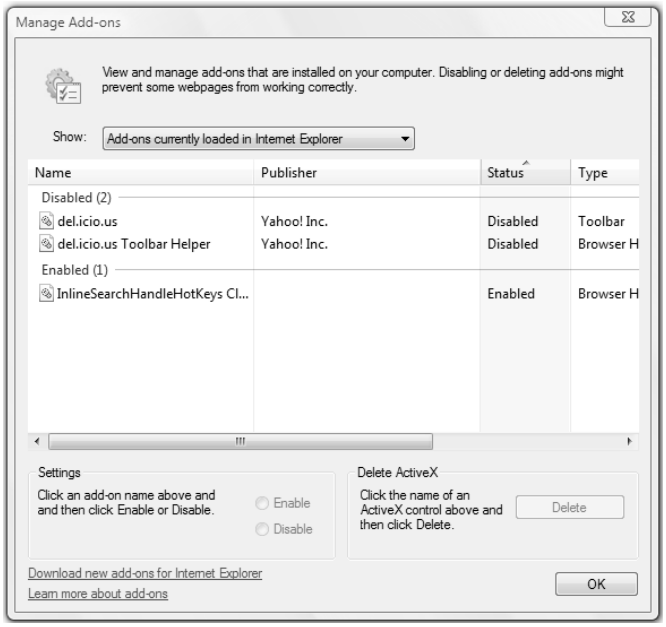
TABLE 9.1 Show List Options of the Manage Add-ons Dialog Box

Option	Description
Add-ons That Have Been Used by Internet Explorer	Displays a complete list of all the add-ons installed in IE
Add-ons Currently Loaded in Internet Explorer	Displays a list of add-ons used for the currently loaded Web page

TABLE 9.1 Show List Options of the Manage Add-ons Dialog Box *(continued)*

Option	Description
Add-ons That Run Without Requiring Permission	Displays a list of add-ons that have been pre-approved by Microsoft
Downloaded ActiveX Controls (32-bit)	Displays a list of ActiveX controls installed on the computer

FIGURE 9.11 The Manage Add-ons dialog box



In some cases, installing third-party add-ons in IE may cause the browser to become unstable or the add-ons may interfere with other applications installed on the computer. To enable you to troubleshoot whether add-ons are causing problems, IE provides the ability to load into Add-ons Disable Mode where only critical system add-ons are loaded. To load IE without loading any installed add-ons, you should click Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Internet Explorer (No Add-ons).

Once you've determined that an add-on is causing IE to become unstable, you can use the Manage Add-ons dialog box to disable the add-on. To disable an add-on, you should open the Manage Add-ons dialog box, select Add-ons That Have Been Used by Internet Explorer in the Show list, select the add-on from the list, and click Disable in the Settings area.

In Exercise 9.3, you will disable an add-on in IE.

EXERCISE 9.3

Disabling an Add-on in IE

1. Select Start ➢ Internet to open Internet Explorer.
2. Click the Tools toolbar item, expand Manage Add-ons, and click Enable or Disable Add-ons.
3. Select the Add-ons That Have Been Used by Internet Explorer item in the Show list to display a list of add-ons installed on your computer.
4. Select an add-on from the list, and click Disable in the Settings area.
5. Click OK.

Configuring Pop-up Blocker

Pop-up Blocker is a feature of IE that prevents pop-ups from being displayed by web pages. Pop-up windows are displayed on top of web pages and are often used by advertisers to display ads to visitors. However, not all pop-ups are advertising-related or malicious. Some web pages display pop-ups to provide useful information.

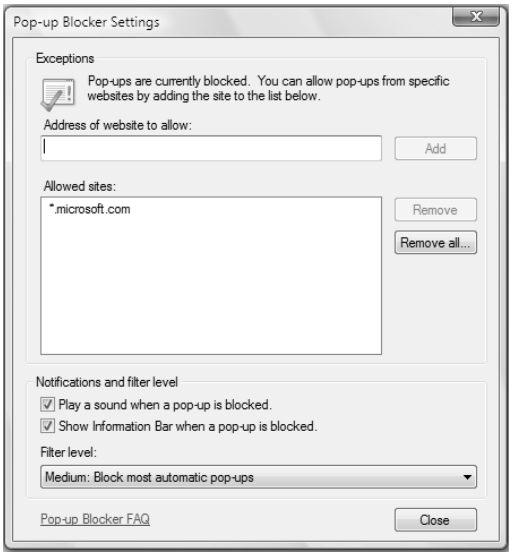
By default, Pop-up Blocker is enabled. When visiting a site that displays pop-ups, a message appears in the Information Bar indicating that a pop-up was blocked. If desired, you can disable Pop-up Blocker by opening IE, clicking the Tools button, expanding Pop-up Blocker, and clicking Turn Off Pop-up Blocker. In the Pop-up Blocker dialog box, click Yes to disable Pop-up Blocker.

Disabling Pop-up Blocker will allow any site to display pop-ups. If you want to enable pop-ups for a few select sites, then you should add those sites to the Allowed Sites list of the Pop-up Blocker Settings dialog box instead of disabling Pop-up Blocker.

To allow a specific site to display pop-ups, you can add that site to a list of sites that are allowed to display pop-ups. To add a site to the list of allowed sites, you should open IE, click the Tools button, expand Pop-up Blocker, and click Pop-up Blocker Settings. The Pop-up Blocker Settings dialog box is displayed, which allows you to enter the address of the site to allow. The Pop-up Blocker Settings dialog box is shown in Figure 9.12.

Alternatively, you can enable pop-ups for a site while the site is displayed in IE. To allow pop-ups when visiting a site where a pop-up was blocked, click the Information Bar and select either the Temporarily Allow Pop-ups option to allow pop-ups during the current visit or the Always Allow Pop-ups from This Site option to allow pop-ups to always be displayed for the website you are visiting. Clicking Always Allow Pop-ups from This Site will add the site to the list of allowed sites in the Pop-up Blocker Settings dialog box.

FIGURE 9.12 The Pop-up Blocker Settings dialog box



In addition to providing the ability to create and maintain a list of approved sites for pop-ups, the Pop-up Blocker Settings dialog box provides the ability to configure notification and filter options. You can enable a sound to be played when a pop-up is blocked and you can enable the Information Bar to be displayed when a pop-up is blocked. The Filter Level drop-down list provides the ability to set the pop-up filter level. The Filter Level drop-down list provides three filter options:

- High: Block All Pop-ups (Ctrl+Alt to override)
- Medium: Block Most Automatic Pop-ups
- Low: Allow Pop-ups from Secure Sites

By default, the Pop-up Blocker Filter Level is set to Medium: Block Most Automatic Pop-ups. In Exercise 9.4, you will add Microsoft.com to the list of approved sites in Pop-up Blocker.

EXERCISE 9.4

Adding a Site to the Allowed Sites List in Pop-up Blocker

1. Select Start ➢ Internet to open Internet Explorer.
2. Click Tools, expand Pop-up Blocker, and click Pop-up Blocker Settings.
3. In the Address of Website to Allow text box, type **microsoft.com** and click Add. The Allowed Sites list will be updated to include `*.microsoft.com`.
4. Click Close.

Security Features of Internet Explorer 7

Internet Explorer 7 contains many security improvements over previous versions of IE. With the increase in malicious attacks over the Web, security was a primary consideration during the development of IE 7. The following list indicates some of the new security improvements in IE:

- A phishing filter to indicate when a site is known or is believed to be fraudulent
- Improved privacy features, allowing you to more easily delete personal information, such as cached passwords, cookies, and form data
- Security Status Bar, which provides detailed security information, such as phishing notifications and certificate names
- Parental controls, which enables parents to proactively control and monitor Internet behavior
- Protected Mode, which isolates IE from other applications and prevents malicious code from being run outside of the Temporary Internet Files location

In the following sections, you will learn about configuring security options in IE.

Configuring Phishing Filter

Phishing is a malicious attack where the attacker attempts to get you to reveal your personal or financial information via an e-mail message or by a seemingly innocuous website. Often, the attacker will send an e-mail message that appears to be from a banking institution or an online retail website indicating that you need to update your information on the sender's site. The e-mail message typically contains a link to what appears to be the website of a legitimate company asking for personal or financial information. However, the website is fraudulent and the personal information is then used for malicious purposes, such as identity theft.

Phishing Filter is a feature of IE 7 that helps identify and notify you if you visit a site that is known to be or believed to be fraudulent. Phishing Filter provides protection against phishing attacks by comparing the visited site against a known list of legitimate sites, analyzing the site for known characteristics of fraudulent sites, and, if desired, sending the website information to Microsoft for further analysis.

Phishing Filter can be configured by opening IE, clicking Tools, and then clicking Phishing Filter. As you can see in Figure 9.13, several options are available on the Phishing Filter menu, including:

- Check This Website
- Turn Off Automatic Website Checking
- Report This Website
- Phishing Filter Settings

The Check This Website option sends the current website address to Microsoft to be checked against a list of known fraudulent websites. If the website is not known to be fraudulent, a message indicating that the website is not a reported phishing website is displayed. If you believe that the website is a phishing website, even though it's not indicated as such, you can report the site by

clicking the Report This Website option of the Phishing Filter menu. If you do not want website information to be automatically sent to Microsoft to be checked for phishing, then you should click the Turn Off Automatic Website Checking option of the Phishing Filter menu. This option will prevent information about websites from being automatically sent to Microsoft. By default, automatic website checking is disabled in Phishing Filter. Clicking the Phishing Filter Settings option of the Phishing Filter menu will open the Internet Options dialog box, as shown in Figure 9.14.

FIGURE 9.13 Phishing Filter menu

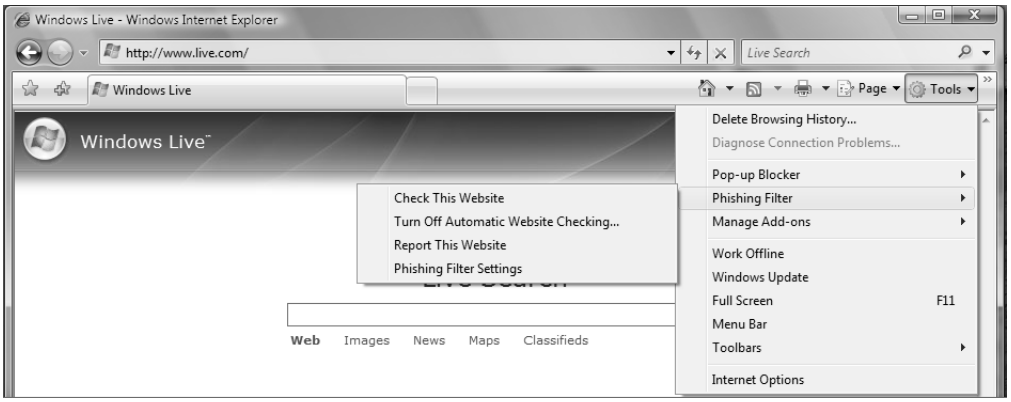
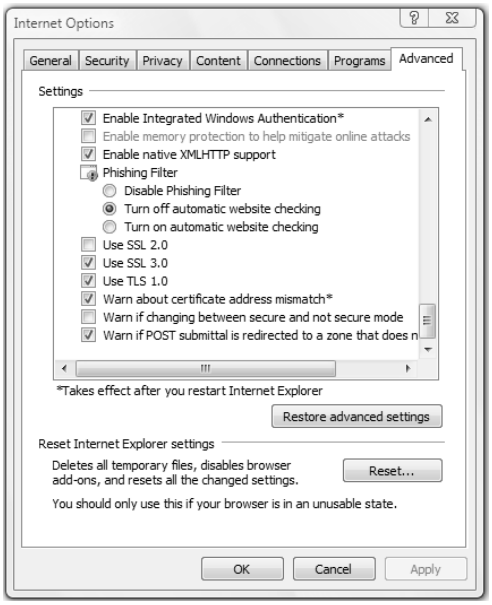


FIGURE 9.14 Advanced tab of the Internet Options dialog box



On the Advanced tab of the Internet Options dialog box, you can disable Phishing Filter, or configure whether automatic website checking should be turned off or turned on. Once the Advanced tab of the Internet Options dialog box is open, you will need to scroll down to the Security area of the Settings list to modify Phishing Filter settings. In Exercise 9.5, you will enable automatic website checking in Phishing Filter.

EXERCISE 9.5

Turn On Automatic Website Checking in Phishing Filter

1. Select Start ➢ Internet to open Internet Explorer.
2. Click Tools, expand Phishing Filter, and click Turn On Automatic Website Checking.
3. Click Turn On Automatic Phishing Filter (recommended) in the Microsoft Phishing Filter dialog box.
4. Click OK.

Configuring Parental Controls

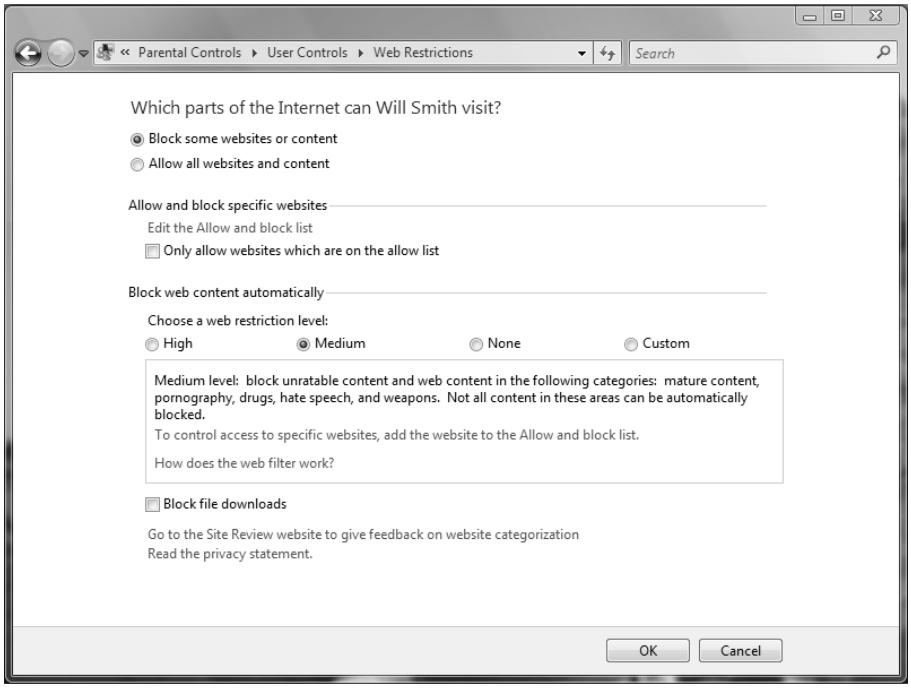
Windows Vista provides improved Parental Controls that enable parents to monitor and control their children's computer behavior, including Internet browsing. Parental Controls enable parents to set limits on when the computer can be used, which programs can be run, which games can be played, and what websites can be viewed. Parental Controls are set on a per-user basis, so if more than one child accesses a computer, then you could provide each child with different access levels on that computer. When a user attempts to visit a website that is blocked by Parental Controls, a message is displayed indicating that the site has been blocked, and the user can request permission to the page or program.

To access Parental Controls in Windows Vista, click Start ➢ Control Panel ➢ User Accounts and Family Safety ➢ Parental Controls. A list of users configured on the computer is displayed. Selecting a Standard User account to which you want to apply Parental Controls will display the Parental Controls dialog box for that user, and you can then click Windows Vista Web Filter to open the Web Restrictions dialog box, as shown in Figure 9.15.

The Web Restrictions dialog box provides you with the ability to allow and block websites, block file downloads, and configure a web restriction level. For example, you can specify which websites the user can access by selecting the Only Allow Websites Which Are on the Allow List option, and then click Edit the Allow and Block List to open the Allow or Block Specific Websites dialog box. Figure 9.16 displays the Allow or Block Specific Websites dialog box.

You can enter the specific websites to allow or block in the Allow or Block Specific Websites dialog box and they will be placed in the Allowed Websites or Blocked Websites lists, based on whether you selected to allow or block the specified website. If the Only Allow Websites Which Are on the Allow List option is selected, then the user will only be able to access sites that are listed in the Allowed Websites list.

FIGURE 9.15 Web Restrictions dialog box

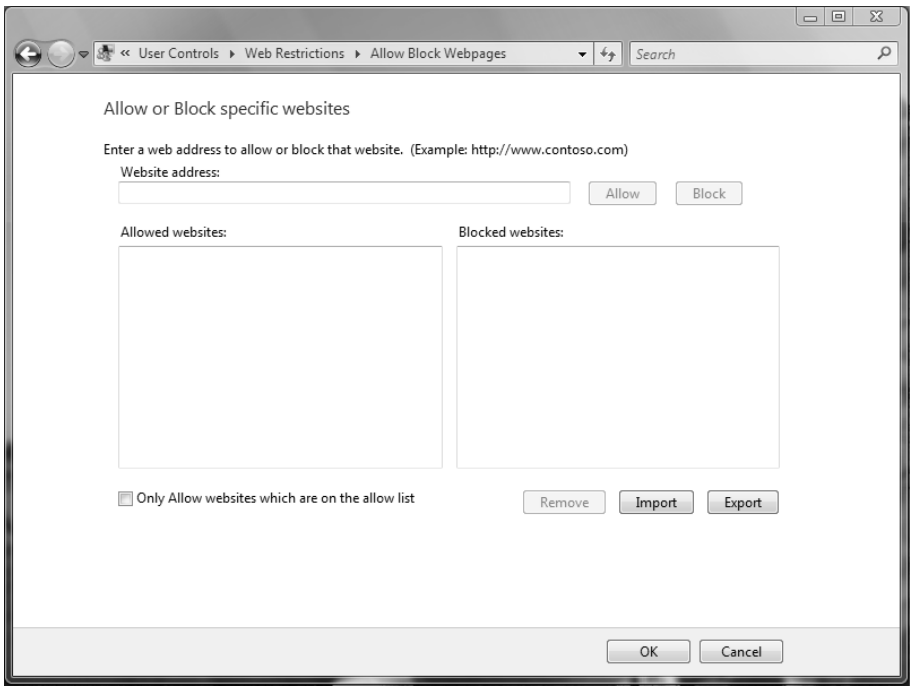


If you want to allow your children to visit sites that are not specifically approved but whose content has been filtered by parental controls, you can configure the Block Web Content Automatically filter. There are four options that you can choose in the Block Web Content Automatically section of the Web Restrictions dialog box. Table 9.2 describes the four content filter options from which you can choose.

TABLE 9.2 Web Content Filter Options

Option	Description
High	Blocks all web content except websites that contain content approved for children
Medium	Blocks content that has not been rated or that is unsuitable for children, including websites that contain mature content, pornography, drugs, hate speech, and weapons
None	Provides no web content filtering
Custom	Allows you to configure the content categories that should be blocked

FIGURE 9.16 Allow or Block Specific Websites dialog box



In Exercise 9.6, you will configure a list of approved sites that a user can visit.

Parental Controls can only be configured by a user with an Administrator user account, and only Standard User accounts can have Parental Controls applied to them.

EXERCISE 9.6

Configure a List of Allowed Sites

1. Click Start ➢ Control Panel ➢ User Accounts and Family Safety ➢ Parental Controls.
2. Select a Standard User account to which you want to apply web filtering.
3. Under Parental Controls, click On, Enforce Current Settings.
4. Click Windows Vista Web Filter.
5. Select Block Some Websites or Content.

EXERCISE 9.6 *(continued)*

6. Click Edit the Allow and Block List to open the Allow or Block Specific Websites dialog box.
7. Type **microsoft.com** into the website address text box, and click Allow. Type any additional websites that you want to allow.
8. Select the Only Allow Websites Which Are on the Allow List option.
9. Click OK until you return to the Parental Controls user list.

Configuring Protected Mode

Protected Mode is a feature of Windows Vista that enables IE to run in a protected, isolated space that prevents malicious code from writing outside of the Temporary Internet Files directory unless specifically granted access by the user. Enabling Protected Mode can help prevent spyware from being installed simply by visiting a website. You are still able to access web pages with Protected Mode enabled, but those web pages will not have access to any of the operating system. You can even install software from the Internet when Protected Mode is enabled, but you must specifically grant the software access to your computer.

To enable Protected Mode, you should click Start ➢ Control Panel ➢ Network and Internet ➢ Internet Options to open the Internet Properties dialog box. Then, click the Security tab and select the Enable Protected Mode (Requires Restarting Internet Explorer) option.

Configuring Privacy

IE 7 provides increased privacy protection that helps keep your personal information private when browsing the Internet. IE also provides increased protection when browsing on a computer where multiple users have access to the computer.

To help protect your personal information, you can configure privacy options on the Privacy tab of the Internet Options dialog box. For example, you can specify the privacy setting for how cookies are handled. In some cases, you may want to allow cookies for the sites you routinely visit, which may allow you to access the site without the need to enter your username and password combination each time. In other cases, you may not want cookies to be stored at all. IE provides several options for how cookies should be handled; these options are described in Table 9.3. By default, IE is configured with the Medium privacy setting.

You can also more granularly configure privacy settings. For example, you can explicitly grant or deny a site the ability to create a cookie on the computer by clicking the Sites button, which opens the Per Site Privacy Actions dialog box. You can enter a site name and select whether to block or allow the site. You can also override the default cookie handling mechanisms of IE by clicking the Advanced button on the Privacy tab of the Internet Options dialog box. The Privacy Tab of the Internet Options dialog box is shown in Figure 9.17.

IE also provides you with the ability to protect personal browsing information that is stored locally on the computer and can be accessed by other users of the computer. For example, through a single interface, you can delete saved form data, browsing history, saved cookies, Temporary Internet Files, and any saved passwords. To delete your browsing history, you should click Start ➢ Internet ➢ Tools ➢ Delete Browsing History, which will open the Delete Browsing History dialog box. In the Delete Browsing History dialog box, you can select to delete all or part of any saved browsing history. For example, if you are using a public computer, you would probably want to delete all saved browsing information. The Delete Browsing History dialog box is displayed in Figure 9.18.

TABLE 9.3 Privacy Options

Option	Description
Block All Cookies	Prevents any cookies from being created, and prevents websites from accessing any cookies that are present on the computer.
High	Prevents websites that do not have a compact privacy policy from storing cookies on the computer. Also prevents cookies from being stored that can allow the website to contact you without your consent.
Medium High	Prevents third-party cookies that do not have a compact privacy policy from being stored on the computer. Also prevents third-party cookies from being stored that can allow the website to contact you without your consent. Prevents first-party cookies that can allow the website to contact you without your consent from being stored on the computer.
Medium	Prevents third-party cookies that do not have a compact privacy policy from being stored on the computer. Also prevents third-party cookies from being stored that can allow the website to contact you without your consent. Restricts first-party cookies that can allow the website to contact you without your consent.
Low	Prevents third-party cookies that do not have a compact privacy policy from being stored on the computer. Restricts third-party cookies that can allow the website to contact you without your consent.
Accept All Cookies	Allows any website to create and store cookies on the computer.

FIGURE 9.17 Privacy tab of Internet Options dialog box

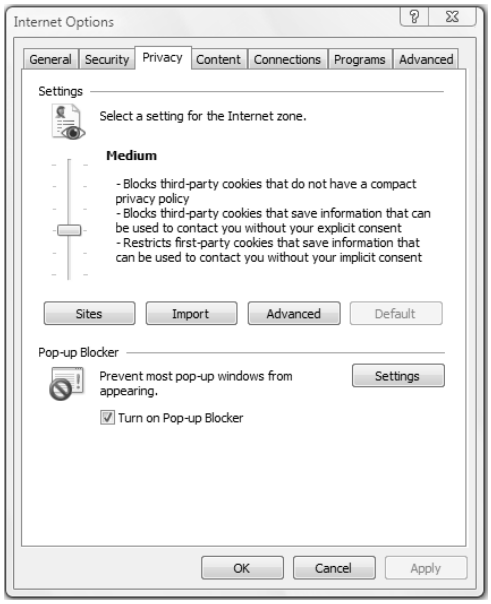


FIGURE 9.18 Delete Browsing History dialog box

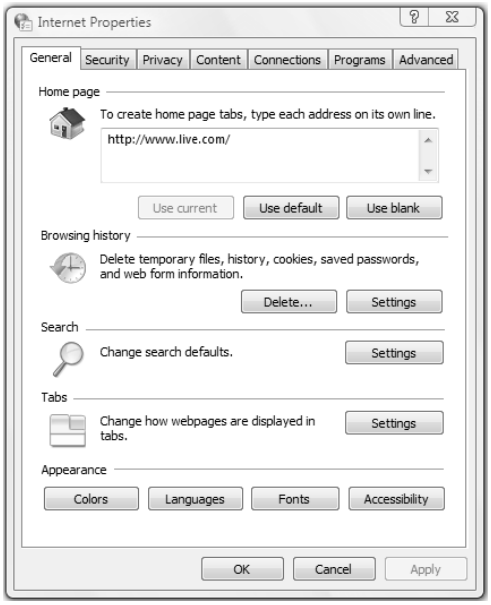
Configuring Internet Explorer Options

In addition to security and usability options that you can configure in IE, you can configure other, more general options. For example, you can specify how web pages are displayed in tabs, which website is used as the home page, AutoComplete settings, which programs are used for e-mail and HTML editing, as well as other advanced settings.

IE settings can be configured by using the Internet Options dialog box. You access Internet Options by right-clicking Internet Explorer from the Start menu and selecting Internet Properties. This brings up the dialog box shown in Figure 9.19.

The Internet Options dialog box contains several tabs: General, Security, Privacy, Content, Connections, Programs, and Advanced. In this section, we'll discuss the General, Security, and Advanced tabs.

FIGURE 9.19 The Internet Options dialog box



Configuring General Options

General properties are used to configure home page, browsing history information, search defaults, and tab information. The Home Page section is used to configure the default home page that is displayed when you launch Internet Explorer. You can specify that you want to

use the current home page for whatever is currently loaded, use the default home page that was preconfigured, or leave the option blank. With IE 7, you can add additional websites to the Home Page area on separate lines, and each website listed will be opened in a new tab each time IE is opened.

The Browsing History section allows you to delete saved browsing information, such as temporary files, history, cookies, saved passwords, and any saved form data. You can configure how much disk space is used to cache web pages, how long sites are saved in the history list, and where the Temporary Internet Files directory is stored.

The Search section allows you to change the default search provider for IE.

The Tabs section allows you to configure options for using the tabbed browsing feature of IE. You can enable or disable tabbed browsing and also configure how and when new tabs should be opened. You can specify whether pop-ups should be opened in a new tab or a new window, and whether links on web pages should be opened in a new tab or a new window.

You can also set other options from the General tab that affect how Internet Explorer is customized, such as colors, fonts, languages, and accessibility options.

Configuring Security Options

The Security tab, as shown in Figure 9.20, allows you to configure the following options:

- The Internet content zones that can be used by the computer
- The local intranet zones that can be used by the computer
- The trusted sites that are allowed for the computer
- The restricted sites that are in effect for the computer

You set security zones by selecting the web content zone you want to configure and then clicking the Sites button. Custom Settings allow you to configure options such as whether you enable the downloading or use of signed or unsigned ActiveX controls and whether .NET Framework components will be allowed to be run. If you have configured your computer for security options and have specified security restrictions, you will receive an error message anytime you access a zone or site that is not configured for use with your computer. You can also enable or disable Protected Mode on the Security tab.

Configuring Advanced Options

The Advanced tab of the Internet Options dialog box, as shown in Figure 9.21, allows you to configure advanced configuration settings for IE, including accessibility settings, browsing settings, encoding settings, multimedia settings, printing settings, and general security settings. For example, you can configure whether links are underlined, whether pictures should be displayed, which version of SSL should be used, whether background colors and images are printed, and many other options.

In addition, the Advanced tab of the Internet Options dialog box allows you to reset any changed settings in IE. The Reset button also deletes any saved temporary files and disables any installed add-ons.

FIGURE 9.20 The Security tab of the Internet Options dialog box

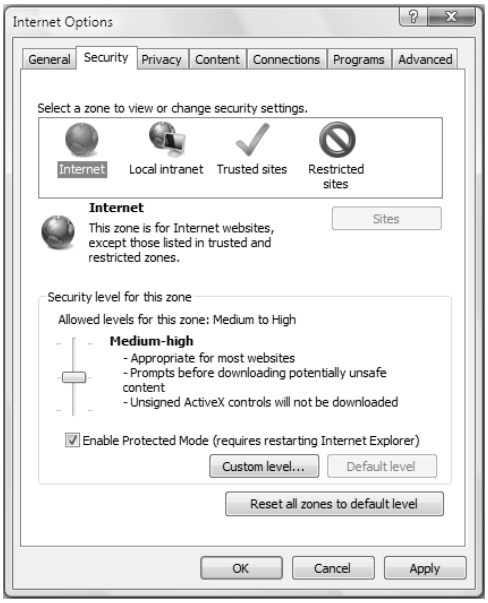
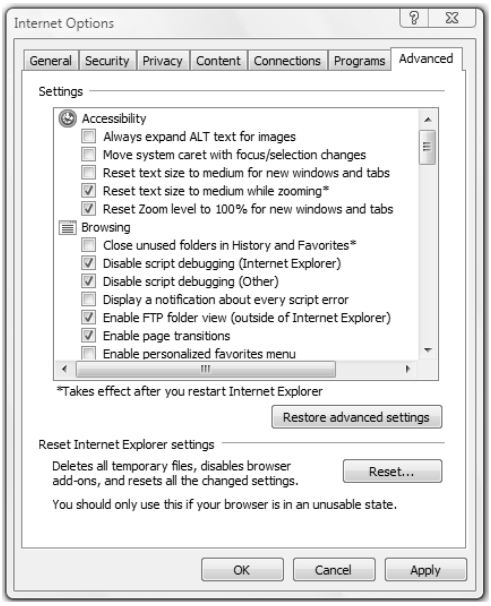


FIGURE 9.21 The Advanced tab of the Internet Options dialog box



Summary

In this chapter, you learned about Internet Explorer and how to configure and manage usability and security options in IE. We covered the following topics:

- IE Instant Search capabilities, including how to configure IE with new search providers, and how to configure search providers as the default search provider in IE
- RSS features of IE, including automatic RSS detection and managing RSS feeds
- IE extensibility features, including how to install add-ons and how to enable or disable add-ons
- Pop-up Blocker, which is used to block pop-ups in web pages
- Phishing Filter, which is used to provide protection against websites attempting to trick you into providing personal and financial information
- Parental controls, which allow you to control and monitor Internet access for children
- Protected Mode, which prevents IE from writing to areas of the operating system unless specifically granted access
- Privacy settings, which allow you to protect your personal information when browsing the Internet
- Internet Options dialog box, from which you can configure general and advanced settings for IE, including security, privacy, and browsing settings

Exam Essentials

Know the options that can be configured for Instant Search. Know how to find and enable search providers. Know how to change the default search provider.

Be able to configure and manage RSS feeds. Know how to configure RSS feed properties, and know how to subscribe to feeds when they are available on a web page.

Know how to configure and manage add-ons. Know how to enable and disable add-ons. Know how to boot IE without add-ons.

Be able to configure Pop-up Blocker. Know how to grant a site the ability to display pop-ups. Know how to enable and disable Pop-up Blocker.

Be able to configure Phishing Filter. Know how to enable and disable Phishing Filter.

Be able to configure Parental Controls. Know how to configure the Web content filter. Be able to edit the Allow and Block list.

Be able to configure Privacy Settings. Know how to enable and disable cookies. Know when it is useful to use cookies, and when cookies should be blocked.

Review Questions

1. You are a help desk technician for your company. You are configuring Internet Explorer, and you want to ensure that cookies that are stored on the computer are not accessible by any websites. Which privacy setting should you configure to accomplish your goal?

   A. Block All Cookies

   B. High

   C. Medium High

   D. Medium

2. You have subscribed to several RSS feeds using Internet Explorer. You discover that one of the websites to which you are subscribed has recently been updated, but the update has not been downloaded to the RSS feed on your computer. What can you do to ensure that you receive the updates in a more timely manner?

   A. Configure the feed to be updated every 4 hours.

   B. Configure attachments to be downloaded automatically.

   C. Increase the number of updates saved in the archive.

   D. Enable the Turn On Feed Reading view option.

3. You monitor several internal websites for your organization. Each day, you need to check various aspects of each site to view updated information. You would like to speed up the process of checking each of these sites. Which of the following could you do?

   A. Enable Quick Tabs.

   B. Configure each site as a Home Page tab.

   C. Add each site to the list of search providers.

   D. Add each site to the Local intranet zone.

4. You are the network administrator for your company. Mark is a user in the finance department and requires access to an FTP site so that he can download financial analysis reports that have been created by a third-party vendor called Finance Data Gurus.

   When Mark attempts to access the FTP server with the URL `ftp://ftp.financedatagurus.com`, Internet Explorer returns the following error message: "The password was rejected."

   Mark informs you that he has a username and password from Finance Data Gurus, but he can't figure out how to provide the username and password. What URL should Mark use to access the FTP site?

   A. `ftp://ftps.financedatagurus.com@Mark:password`

   B. `ftp://ftp.financedatagurus.com/Mark:password`

   C. `ftp://Mark:password@ftp.financedatagurus.com`

   D. `ftps://ftp.financedatagurus.com/Mark:password`

5. You want to configure Wikipedia.org as the search provider used for Instant Search in Internet Explorer. How can you accomplish this?
   - **A.** Configure Wikipedia.org as your home page.
   - **B.** Configure the Wikipedia.org search provider as the default search provider.
   - **C.** Type **Wikipedia.org** into the Instant Search box.
   - **D.** Configure Wikipedia.org in the list of Allowed Sites.

6. You visit a website that appears to be from a banking institution. However, before you enter your financial information, you want to verify that the site is not fraudulent. What can you do?
   - **A.** Verify that the site is using SSL.
   - **B.** Click the Report This Site option on the Phishing Filter menu.
   - **C.** Click the Check This Site option on the Phishing Filter menu.
   - **D.** Click the Verify This Site option on the Phishing Filter menu.

7. Your company publishes an RSS feed accessible only to employees that is updated with company information, such as general company news and HR information. You have subscribed to the feed using Internet Explorer, and now you want to view the information in the RSS feed. Which of the following should you do?
   - **A.** Type in the URL of the company website offering the RSS feed and view the information from that site.
   - **B.** Access the Favorites Center.
   - **C.** Open the RSS feed using an XML editor.
   - **D.** Click the orange icon on the toolbar in Internet Explorer.

8. You have recently installed Windows Vista on your computer. You are configuring Internet Explorer, and you want to ensure that cookies are not saved from any website that does not have a compact privacy policy. Which privacy setting should you configure to accomplish your goal?
   - **A.** Block All Cookies
   - **B.** High
   - **C.** Medium High
   - **D.** Medium

9. Your network administrator has provided you with a new laptop with Windows Vista installed on it. You are using Internet Explorer. When typing search phrases into the Instant Search box, you discover that search results are only being displayed for Amazon.com. You want search phrases to search the Web, not Amazon.com. What should you do?
   - **A.** Disable all add-ons.
   - **B.** Configure Internet Explorer as your default browser.
   - **C.** Configure a web-based search provider as your default search provider.
   - **D.** Configure a web-based search provider as your default home page.

10. You have downloaded and installed several Internet Explorer add-ons. You want to view the add-ons that have been used during your current browsing session. Which option of the Manage Add-ons dialog box should you select to view this information?
    A. Add-ons That Have Been Used by Internet Explorer
    B. Add-ons Currently Loaded in Internet Explorer
    C. Add-ons That Run Without Requiring Permission
    D. Downloaded ActiveX Controls (32-bit)

11. You want to ensure that your daughter Samantha, who is 8 years old, is not presented with any objectionable material while surfing the Web. You are configuring Parental Controls to filter out any objectionable content. What web restriction level should you configure?
    A. High
    B. Medium
    C. Low
    D. None

12. You have recently provided your password to a fraudulent website by accident. You want to protect against this happening again in the future. Which of the following features of Internet Explorer should you enable to accomplish your goal?
    A. Pop-up Blocker
    B. Parental Controls
    C. Protected Mode
    D. Phishing Filter

13. Your computer is used by several members of your family, including your children. You want to ensure that any content discussing drugs, pornography, and weapons will not be displayed for your children's user accounts. You are configuring Parental Controls to filter out this objectionable content. What web restriction level should you configure?
    A. High
    B. Medium
    C. Low
    D. None

14. You have downloaded and installed several add-ons to Internet Explorer. Internet Explorer will no longer start, and you suspect that one of the add-ons is causing Internet Explorer to become unstable. You need to start Internet Explorer and connect to the Internet in order to research the add-on to determine if there are any known issues with it. Which of the following should you do?
    A. Reinstall Internet Explorer.
    B. Disable all of the installed add-ons.
    C. Delete all of the installed add-ons.
    D. Open Internet Explorer without add-ons.

15. You want to monitor the websites visited by other users of your computer. Which of the following features of Internet Explorer should you enable to accomplish your goal?

A. Add-on Manager

B. Parental Controls

C. Protected Mode

D. Phishing Filter

16. You want to ensure that your children are only able to view websites to which you specifically grant them access. You are configuring Parental Controls to accomplish this. What should you do? (Choose all that apply.)

A. Set the web restriction level to Medium.

B. Edit the Allow list to include the websites you want to allow your children to visit.

C. Select the Only Allow Websites Which Are on the Allow List option.

D. Select the Block File Downloads option.

E. Select the Block Some Websites or Content option.

17. You recently visited a website that automatically downloaded and installed spyware onto your computer. You want to prevent spyware from being installed in the future. You have enabled Pop-up Blocker. What else can you do to minimize your risk of downloading spyware?

A. Enable Phishing Filter.

B. Disable all add-ons.

C. Delete your browsing history.

D. Enable Protected Mode.

18. You share a computer with three other people. You discover that one of the other users can view the websites that you recently visited. You want to prevent the other computer users from being able to view this information. Which of the following should you do?

A. Configure your user account with Administrator access.

B. Set the privacy settings to High.

C. Delete the browsing history.

D. Delete the Temporary Internet Files folder.

19. You have recently downloaded an ActiveX control onto your computer. Shortly after downloading the control, Internet Explorer occasionally crashes. You need to prevent Internet Explorer from crashing. Which of the following should you do?

A. Isolate the ActiveX control by using Protected Mode.

B. Add the ActiveX control to the Block list.

C. Disable the ActiveX control.

D. Add the ActiveX control to the trusted sites zone.

20. You are responsible for purchasing computer equipment for your organization. You typically purchase equipment from an online supplier. The online supplier's website displays a pop-up window with the details of the transaction after you complete a purchase. However, you've enabled Pop-up Blocker and the pop-up is blocked. You need to view this pop-up in order to get the details of the transaction, and you need to ensure that similar pop-ups on the online supplier's site are not blocked in the future. What should you do?

A. Disable Pop-up Blocker.

B. Add the online supplier's website to the Allowed Sites list.

C. Temporarily allow pop-ups for the site.

D. Set the Filter level option to Low.

Answers to Review Questions

1. A. To block any website from accessing cookies stored on the local computer, you should set the privacy setting to Block All Cookies. The Block All Cookies setting prevents cookies from being saved on the computer, and prevents any existing cookies from being read by websites.

2. A. You should configure the feed to be updated more often in order to receive updates in a more timely manner. By default, RSS feeds in IE are updated once per day. However, you can modify the default schedule or create a custom schedule. Feeds can be configured to be updated every 15 minutes, every 30 minutes, every hour, every 4 hours, once a day, once a week, or never.

3. B. You could configure each of the sites that you need to monitor as a Home Page tab. You can configure multiple websites as Home Page tabs. Each time you open Internet Explorer, every site that is configured as a Home Page tab will be opened in a separate tab. Consequently, if you check multiple sites a day, adding each of the sites to the Home page area will speed up the process because you will not have to type in each of the sites' addresses, and all of the sites will be opened automatically.

4. C. If you need to provide logon credentials as a part of the FTP request, then the syntax you would use would be `ftp://username:password@company.com`.

5. B. You should configure the Wikipedia.org search provider as the default search provider for Instant Search in Internet Explorer. You can add search providers to Internet Explorer, and those search providers can be used by the Instant Search feature of Internet Explorer. When a new default search provider is configured, the new default search provider will be used for each search request entered into the Instant Search box.

6. C. You should click the Check This Site option on the Phishing Filter menu. Phishing Filter provides protection against fraudulent sites by checking sites against a database of known fraudulent sites. Phishing Filter also checks the site to determine whether the site uses known phishing characteristics. The Report This Site option can be used to report a site to Microsoft that you believe is fraudulent. To report a site or check a site, you can access the Phishing Filter menu by opening Internet Explorer, clicking Tools, and expanding the Phishing Filter menu.

7. B. To view RSS feeds to which you are subscribed, you should access the Feeds section of the Favorites Center. When subscribing to RSS feeds using Internet Explorer, those feeds are added to the Favorites Center. To access the Favorites Center, open Internet Explorer, click the Star icon, and then click Feeds.

8. B. To block cookies from any websites that do not have a compact privacy policy, you should set the privacy setting to High. The High setting prevents any cookies from being saved for websites that do not contain a compact privacy policy, and prevents any cookies from being saved that have the potential of saving information that can be used to contact you without your explicit consent.

9. C. You should configure a web-based search provider as your default search provider. The Instant Search box provides a quick method for searching for information. Instant Search supports various search providers, such as Windows Live Search, Google, Yahoo, Amazon.com, and many more. You can also create your own search provider. Once configured as the default search provider, the selected search provider will be used by default for any phrases entered in the Instant Search box.

10. B. A list of add-ons that have been used by Internet Explorer during the current browsing session can be view by selected the Add-ons Currently Loaded in Internet Explorer option of the Manage Add-ons dialog box. You can use the Manage Add-ons dialog box to view, enable, and disable add-ons that have been installed on your computer. To access the Manage Add-ons dialog box, open Internet Explorer, click Tools, click Manage Add-ons, and click Enable or Disable Add-ons.

11. A. You should set the web restriction level to High in Parental Controls for Samantha's user account. Parental controls enable you to control and monitor the content that your child can view. The High web restriction level blocks all content except for content explicitly approved for children.

12. D. You should enable Phishing Filter. Phishing Filter provides protection against fraudulent sites attempting to gain access to your personal or financial information. Phishing Filter checks websites to determine whether they are fraudulent or use characteristics common to phishing attacks.

13. B. You should set the web restriction level to Medium in Parental Controls for each of your children's user accounts. Parental controls enable you to control and monitor the content that your children can view. The Medium web restriction level blocks unratable content, pornography, drug content, hate speech, and weapon-related content.

14. D. You should open Internet Explorer without add-ons by clicking Start ➢ All Programs ➢ Accessories ➢ System Tools ➢ Internet Explorer (No Add-ons). This will start Internet Explorer without any of the installed add-ons being loaded, which will enable you to determine if an add-on is the cause of the problems and will allow you to connect to the Internet to research whether any of the add-ons have known issues.

15. B. You should enable Parental Controls for each of the user accounts that you want to monitor. Parental Controls provide you with the ability to control and monitor which websites your children access. You can configure a list of the websites that you want to allow your children to visit, and you can configure a list of websites that should be blocked. Additionally, you can filter content based on the type of content being displayed.

16. B, C, E. To grant your children access to only sites that you approve, you should perform the following tasks: edit the Allow list to include the websites you want to allow your children to visit, select the Only Allow Websites Which Are on the Allow List option, and select the Block Some Websites or Content option on the Parental Controls Web Restrictions dialog box. Parental Controls allow you to control and monitor which sites your children can access. You can set a web restriction level that automatically filters content, or you can explicitly configure websites that your children can visit.

17. D. You should enable Protected Mode. Protected Mode isolates Internet Explorer and prevents information from being written outside of the Temporary Internet Files unless you allow it. By enabling Protected Mode, you will be prompted before any application is able to write to other areas of the operating system. To enable Protected Mode, open Internet Explorer, click Tools, click Internet Options, click the Security tab, and select the Enable Protected Mode option.

18. C. You should delete your browsing history by clicking the Delete All button or the Delete history button on the Delete Browsing History dialog box. The Delete Browsing History dialog box provides the ability to quickly delete any browsing history, such as the list of websites that you have visited, any cookies that have been stored, saved passwords, and any saved form data. To access the Delete Browsing History dialog box, open Internet Explorer, click Tools, and click Delete Browsing History.

19. C. You should disable the ActiveX control. It is likely that the ActiveX control is causing Internet Explorer to crash. Downloading components from untrusted sources can cause Internet Explorer to become unstable. Disabling the control prevents it from being loaded into IE and will allow you to determine whether the ActiveX control is causing Internet Explorer to crash.

20. B. To allow the online supplier's website to display pop-ups, you should add the website to the list of Allowed Sites on the Pop-up Blocker Settings dialog box. To access the Pop-up Blocker Settings dialog box, you can click Start, open Internet Explorer, click Tools, click Pop-up Blocker, and click Pop-up Blocker Settings. Alternatively, you can allow a site to display pop-ups by clicking the Information Bar when a pop-up is blocked and selecting Always Allow Pop-ups from This Site or Temporarily Allow Pop-ups, depending on whether you want to always view pop-ups on the site or just during the current visit.

Chapter

10

Configuring Windows Vista Applications

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Configuring Applications Included with Windows Vista**
  - Configure and troubleshoot media applications
  - Configure Windows Mail
  - Configure Windows Meeting Space
  - Configure Windows Calendar
  - Configure Windows Fax and Scan
  - Configure Windows Sidebar

Windows Vista offers many new and upgraded applications and tools. In addition to Internet Explorer 7, which we covered in Chapter 9, "Configuring Internet Explorer," Windows Vista also includes the following applications and tools:

- Welcome Center
- Windows Sidebar
- Windows Mail
- Windows Contacts
- Windows Calendar
- Windows Fax and Scan
- Windows Meeting Space
- Windows SideShow
- Windows Sync Center
- Windows Games Explorer

New and updated media tools are also available, including the following:

- Windows Media Player 11
- Windows Media Center
- Windows Photo Gallery
- Windows Movie Maker 6
- Windows DVD Maker

This chapter will cover how to use and configure many of these new and upgraded applications and tools found in Windows Vista.

There are also many new tools available to help maintain and optimize Windows Vista. We will discuss these tools in Chapter 11, "Maintaining and Optimizing Windows Vista."

Applications Removed from Windows Vista

Some applications that were found in Windows XP have been removed or have been made redundant by replacement applications in Windows Vista. The following applications and services are no longer available in Windows Vista:

- Windows Messenger and the Messenger Service
- HyperTerminal
- MSN Explorer
- NetMeeting
- Outlook Express

Although the Telnet client, `telnet.exe`, is not installed by default, you can manually install it by clicking Start ➢ Control Panel ➢ Programs ➢ Turn Windows Features On or Off and then selecting Telnet Client.

Using Welcome Center

The *Welcome Center*, shown in Figure 10.1, launches automatically by default after you log in to Windows Vista. Alternatively, you can access the Welcome Center by clicking Start ➢ Control Panel ➢ System and Maintenance ➢ Welcome Center.

The top of the window displays the installed edition of Windows Vista, the CPU, the amount of RAM, the video card, and the computer name. Below this section are two subsections: Get Started with Windows and Offers from Microsoft. The bottom of the window contains a check box where you can select whether you want the Welcome Center to launch at startup.

Clicking Show More Details will launch the System dialog box, shown in Figure 10.2. This is the same dialog box that appears when you click Start ➢ Control Panel ➢ System and Maintenance ➢ System, or when you right-click Computer and select Properties. In addition to the information presented in the Welcome Center, the System dialog box displays the following information:

- Windows Experience Index
- Operating System Type (32-bit or 64-bit)

- Computer Description
- Workgroup or Domain name
- Activation Status
- Product ID

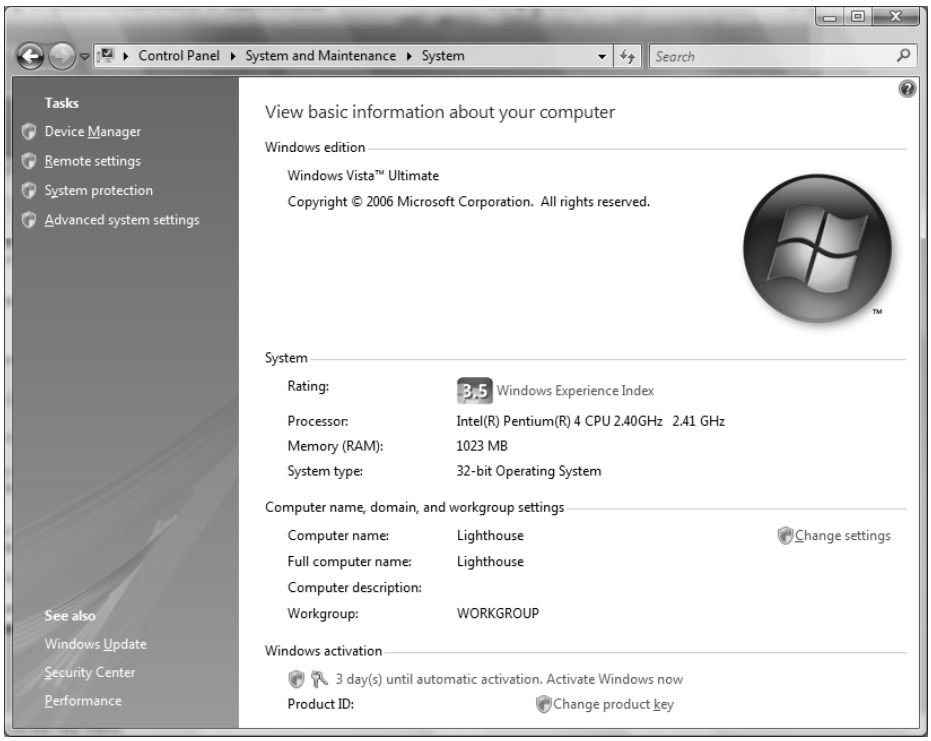
We'll cover the Windows Experience Index in Chapter 11.

Get Started with Windows

The Get Started with Windows section of the Welcome Center contains icons that enable you to perform common tasks quickly and easily. The installation shown in Figure 10.3 contains 14 icons in this subsection. To view the entire list, click Show All 14 Items. A single click on an icon will provide information about the icon; a double-click will launch the associated application.

FIGURE 10.1 Welcome Center dialog box

FIGURE 10.2 System dialog box



The icons include the following:

View Computer Details A single click displays information about your computer at the top of the window; a double-click opens the System dialog box (discussed in the previous section).

Transfer Files and Settings This launches Windows Easy Transfer.

Add New Users This launches User Accounts and Family Safety, where you can add user accounts and set up Parental Controls.

Connect to the Internet This launches the Connect to the Internet wizard.

Windows Ultimate Extras This launches Windows Update to download Windows Ultimate Extras, which are programs and services that are only available with Windows Vista Ultimate.

What's New in Windows Vista This launches a Windows Help and Support window that explains the new features in Windows Vista.

Personalize Windows This launches the Personalization dialog box, where you can change your window color, desktop background, screen saver, sounds, mouse pointers, theme, display settings, icons, and font size.

FIGURE 10.3 Get Started with Windows

Register Windows Online This launches Internet Explorer and directs you to the Windows Vista Registration website.

Windows Media Center This launches *Windows Media Center*, where you can watch or record TV, watch DVDs and videos, listen to music, and view and edit photos.

Windows Basics This launches a Windows Help and Support window that explains the basics of how to use Windows Vista, including how to use a mouse, a keyboard, and the basic features that come with Windows Vista.

Ease of Access Center This launches the Ease of Access Center, where you can configure settings that make your computer easy to use, especially for users with disabilities.

Back Up and Restore Center This launches the *Back Up and Restore Center*, which can be used to back up or restore individual files or an image of the entire computer.

Windows Vista Demos This launches a Windows Help and Support window that contain links to video-based demos that explain how to perform certain tasks in Windows Vista.

Control Panel This launches the Control Panel dialog box.

We discuss Windows Easy Transfer in Chapter 1, "Getting Started with Windows Vista." We explore personalization and the Ease of Access Center in Chapter 4, "Configuring the Windows Vista Desktop." User Accounts are discussed in Chapter 5, "Configuring Users and Groups." We discuss Windows Media Center later in this chapter, and we examine the Back Up and Restore Center in Chapter 11, "Maintaining and Optimizing Windows Vista."

Offers from Microsoft

This subsection of the Welcome Center contains icons that link to online sites. These sites contain information about Microsoft applications that you might be interested in purchasing. Our example installation contains seven icons in this subsection, as shown in Figure 10.4. Similar to the previous subsection, a single click on an icon will provide information about the icon; a double-click will launch Internet Explorer and take you to the appropriate website.

The icons include the following:

- Go Online to Learn About Windows Live contains information about Windows Live, which is a set of services offered by Microsoft that enable you to do the following:
  - Find information quickly with Live Search, Live.com, Windows Live Expo, and Windows Live Toolbar.

FIGURE 10.4 Offers from Microsoft

  - Communicate with friends and family with Windows Live Messenger, Windows Live Mail, and Windows Live Spaces.
  - Protect your computer with Windows Live OneCare.
  - Gain access to information with Windows Live Favorites, Windows Live Alerts, Windows Live Custom Domains, and Windows Live for Mobile.
- Go Online to Find It Fast with Windows Live contains information about Live Search, Live.com, and Windows Live Toolbar.
- Go Online to Help Protect Your PC with Windows Live contains information about Windows Live OneCare.
- Go Online to Windows Marketplace launches the Windows Marketplace website, where you can purchase and download software, as well as purchase hardware and devices.
- Go Online to Connect and Share with Windows Live contains information about Windows Live Messenger, Windows Live Mail, and Windows Live Spaces.
- Go Online to Find More Ways to Help Protect Your PC contains information about third-party antivirus providers for Windows Vista.
- Sign Up Online for Technical Support launches Microsoft's Help and Support website, where you can get support for Microsoft's operating systems, applications, and hardware devices.

We won't discuss Windows Live and Windows Marketplace in detail in this study guide.

Using Windows Sidebar

The *Windows Sidebar*, which was covered in Chapter 4, is a new feature of Windows Vista that can be displayed on the side of your desktop. The Windows Sidebar contains *gadgets*, which provide quick, visual representations of information. The gadgets that are included by default in Windows Vista include the following:

- Calendar
- Clock
- Contacts
- CPU Meter
- Currency

- Feed Headlines
- Notes
- Picture Puzzle
- Slide Show
- Stocks
- Weather

To add a gadget, right-click the Sidebar and select Add Gadgets or click the plus sign (+) at the top of the Sidebar. The Gadgets window, shown in Figure 10.5, will appear. You can find out information about a gadget by clicking a gadget icon and clicking Show Details. You can also get more gadgets online by clicking Get More Gadgets Online. Double-clicking a gadget will add it to the Sidebar. If the Sidebar fills up with gadgets, a second column of gadgets will appear, and you can use the left and right arrows to scroll horizontally through them.

When you hover over a gadget, icons appear in the upper-right corner of the gadget. To remove a gadget, click the X in the upper-right corner. To configure a gadget, click the wrench icon in the upper-right corner. To move a gadget, click and drag the dotted area in the upper-right corner. Right-clicking on a gadget enables you to detach the gadget from the Sidebar (so that you can place the gadget on the desktop) and adjust the opacity (how transparent or opaque the gadget is).

If a gadget is underneath a window, you can bring all of the gadgets to the foreground by right-clicking the Sidebar and selecting Bring Gadgets to Front. If the Sidebar is preventing access to an application or desktop icons, right-click the Sidebar, select Properties, and deselect Sidebar Is Always on Top of Other Windows. Finally, to close the Sidebar, right-click it and select Close Sidebar.

In Exercise 10.1, you will add a gadget to the Sidebar, then place it on the Desktop.

FIGURE 10.5 Windows Sidebar Gadgets

EXERCISE 10.1

Adding a Gadget to the Desktop

1. If the Sidebar is not already active on your desktop, right-click the Windows Sidebar icon in the taskbar and select Open. If the icon is not available, click Start ➢ All Programs ➢ Accessories ➢ Windows Sidebar.
2. Right-click an open area of the Sidebar and select Add Gadgets, or click the plus sign (+) at the top of the Sidebar.
3. Add a gadget to the Sidebar by double-clicking on its icon.
4. Place the gadget on the Desktop by right-clicking the gadget and selecting Detach from Sidebar, or by clicking and dragging the dotted area in the upper-right corner of the gadget.

Using Windows Mail

Windows Mail has replaced Outlook Express in Windows Vista. However, the engine is basically the same as Outlook Express, with a few new features added in. Junk e-mail and phishing filters have been enabled. Finally, Windows Mail Communities enables you to easily access newsgroups.

When you launch Windows Mail for the first time, you will be prompted to configure your e-mail account information. After that is complete, Windows Mail will launch, as shown in Figure 10.6.

Configuring Windows Mail

Windows Mail can do everything Outlook Express can do. You can add and delete e-mail accounts, create message rules, and configure advanced options. You can also import and export contacts, messages, and account settings.

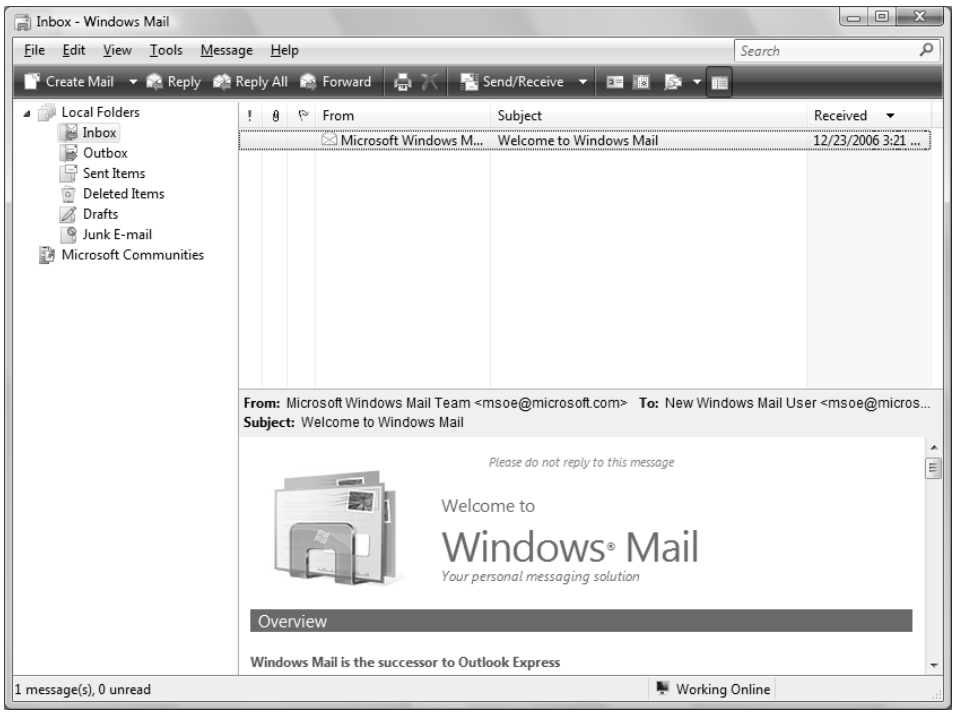
Configuring E-mail Accounts

Configuring e-mail accounts in Windows Mail is easy. To add, delete, or modify an account, click Tools ➢ Accounts. The Internet Accounts window will be displayed, as shown in Figure 10.7. To add an account, click Add; to delete an account, select the account and click Remove. You can change account settings by selecting the account and clicking Properties.

To add an e-mail account, follow these steps:

1. You will be prompted to select the type of account you would like to add. You can add an e-mail account, a newsgroup account, or a directory service. Click E-mail Account to create an e-mail account, then click Next.

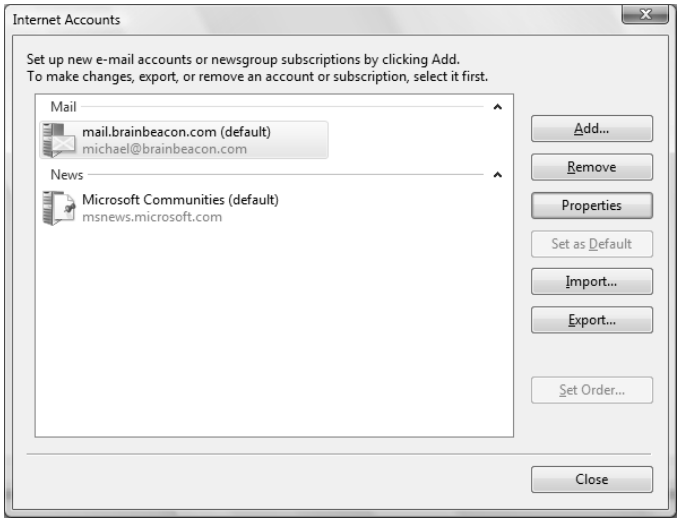
FIGURE 10.6 Windows Mail



2. You will be prompted for a display name. Type the name that you would like others to see when you send them an e-mail message, then click Next.
3. You will be prompted for the e-mail address. Type the e-mail address and click Next.
4. You will be prompted for the e-mail server type, the incoming mail server, and the outgoing mail server. Windows Mail supports the use of *Post Office Protocol 3 (POP3)* and *Internet Message Access Protocol (IMAP or IMAP4)* for incoming mail, and *Simple Mail Transfer Protocol (SMTP)* for outgoing mail. You can specify the e-mail server by name or by IP address. You can also select whether your SMTP server requires authentication. Enter all of the required information and click Next.

Hypertext Transfer Protocol (HTTP) mail, such as Hotmail, is no longer supported in Windows Mail. Microsoft recommends using the Windows Live Mail desktop client for web-based mail such as Hotmail and MSN Mail.

FIGURE 10.7 Internet Accounts dialog box



5. You will be prompted for your e-mail account name and your password. Typically, this is the same as the username in front of the @ sign in your e-mail address. However, some service providers require that you use your full e-mail address as your account name. If you want Windows Mail to remember your password, select the Remember Password check box. Enter your e-mail account name and password, then click Next.
6. Finally, you will be asked whether you want to download your e-mail at this time. If you do not want to download it now, select the check box and click Finish. Otherwise, just click Finish.

After you have created an e-mail account, you can modify the account settings by selecting the e-mail account and clicking Properties. The General tab, shown in Figure 10.8, is used to change the name that you use to identify your e-mail account on your computer, your display name, your e-mail address, and whether Windows Mail will automatically receive mail for this account.

The Servers tab, shown in Figure 10.9, is used to change the incoming and outgoing server names, your e-mail username, and your password. You can also select whether your password is remembered by Windows Mail. Secure Password Authentication and SMTP server authentication can also be configured.

FIGURE 10.8 E-mail account Properties, General tab

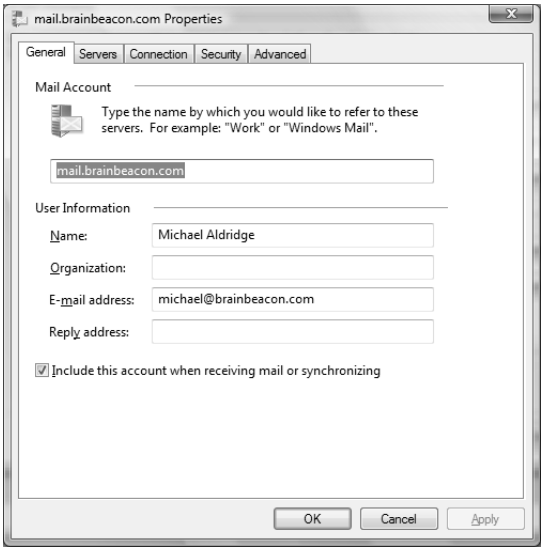
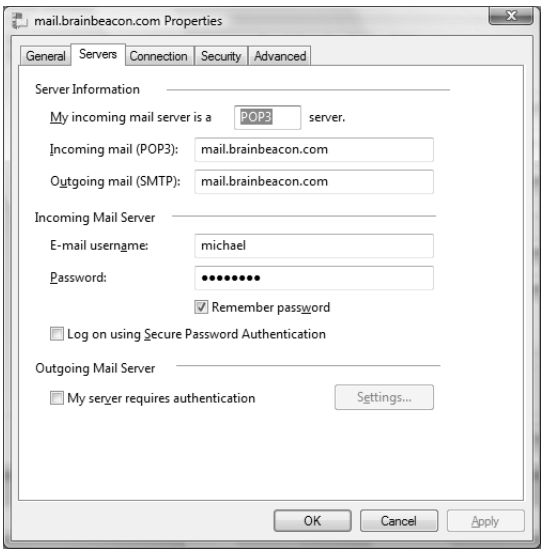


FIGURE 10.9 E-mail account Properties, Servers tab



The Connection tab, shown in Figure 10.10, is used to specify whether you need to connect by using a particular connection, such as your LAN connection or a dial-up connection. The default connection setting is found in Internet Explorer.

The Security tab, shown in Figure 10.11, is used to configure certificates and encryption. The following encryption algorithms are supported by Windows Mail, and are ordered from most secure to least secure:

- Triple Data Encryption Standard (3DES), 168-bit encryption
- Rivest Cipher 2 (RC2), 128-bit encryption
- RC2, 64-bit encryption
- Data Encryption Standard (DES), 56-bit encryption
- RC2, 40-bit encryption

The Advanced tab, shown in Figure 10.12, is used to configure incoming and outgoing port numbers, server timeouts, and whether long messages are broken apart. You can also configure POP3 accounts to leave a copy of messages on the server. By default, the following ports are used for incoming and outgoing mail:

- SMTP: 25
- POP3: 110
- Secure POP3: 995
- IMAP: 143
- Secure IMAP: 993

FIGURE 10.10 E-mail account Properties, Connection tab

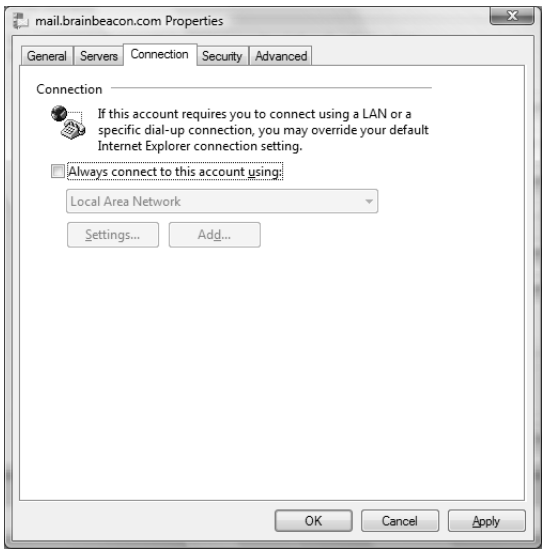


FIGURE 10.11 E-mail account Properties, Security tab

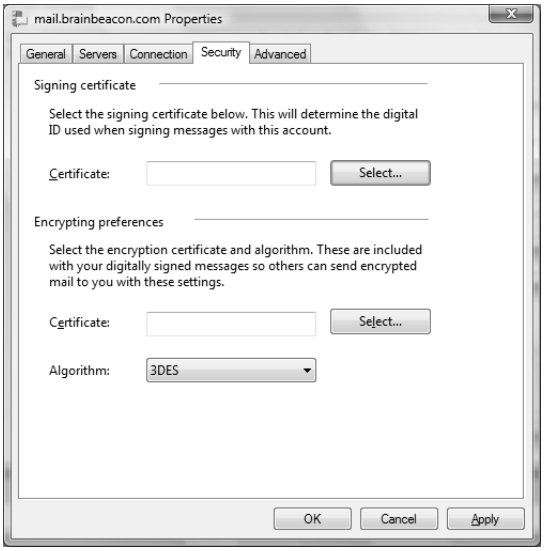
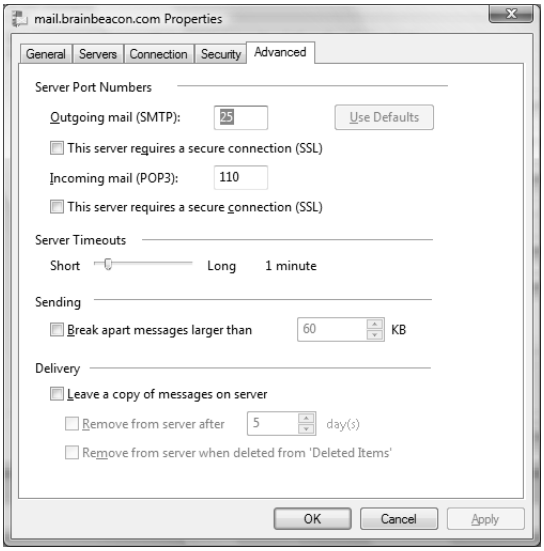


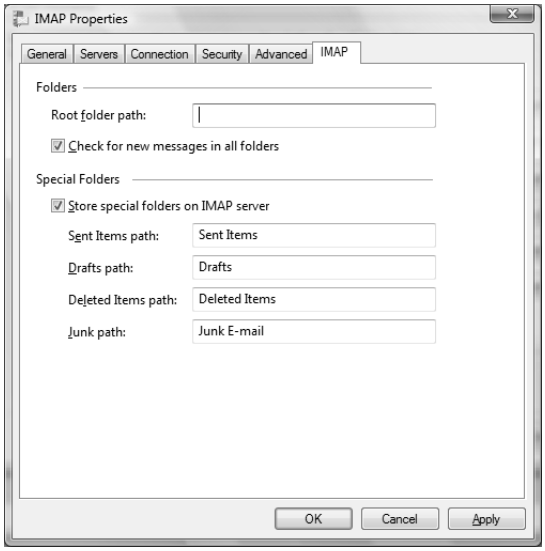
FIGURE 10.12 E-mail account Properties, Advanced tab



The IMAP tab, shown in Figure 10.13, is used to configure IMAP-specific functionality. This tab will not be displayed for POP3 accounts. You can choose to check for new messages in all folders, and configure where you want to store certain types of e-mail messages.

In Exercise 10.2, you will add a POP3 e-mail account.

FIGURE 10.13 E-mail account Properties, IMAP tab



EXERCISE 10.2

Adding an E-mail Account

1. In Windows Mail, click Tools ➢ Accounts.
2. The Internet Accounts window will be displayed. Click Add.
3. Select E-mail Account and click Next.
4. Type the name that you would like others to see when you send an e-mail message, then click Next.
5. Type your e-mail address and click Next.
6. Select your server type and type the name or IP address of your incoming and outgoing e-mail servers. If your SMTP server requires authentication, select the check box. Then, click Next.
7. Type your e-mail username and password, then click Next.
8. Click Finish. Your e-mail messages will begin downloading to Windows Mail.

Creating Message Rules

Message rules are used to automatically perform actions on e-mail and newsgroup messages based on certain conditions. For example, you can configure Windows Mail to perform the following actions:

- Move messages from a particular e-mail address or domain name to a folder.
- Delete messages from a particular e-mail address or domain name.
- Forward messages that contain specific words in the message body.
- Flag messages that are marked as priority.
- Automatically reply to messages that contain specific words in the Subject line.

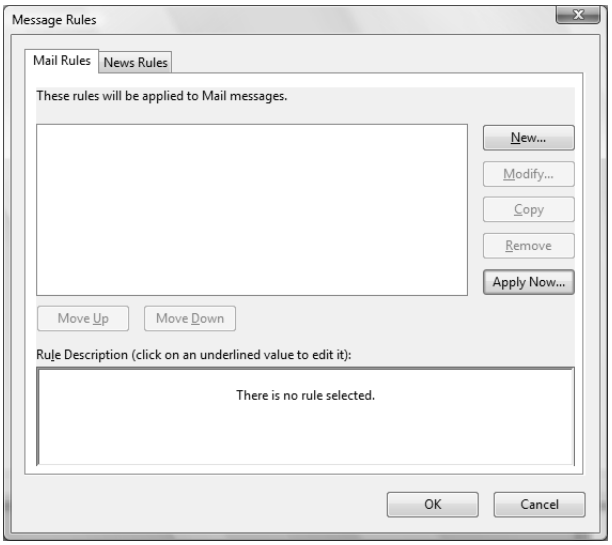
Every rule contains one or more conditions and one or more actions. You can combine multiple conditions and multiple actions. For example, you can configure a rule to forward only large messages from a certain person, and then delete the message.

To add, delete, copy, modify, or prioritize message rules, click Tools ➢ Message Rules ➢ Mail. The Message Rules dialog box, shown in Figure 10.14, will be displayed.

Message rules are processed in a certain order. Rules that are ordered higher in the list will be processed first. To increase a rule's priority by moving it up the list, select the rule and click Move Up. To decrease a rule's priority, select the rule and click Move Down.

If e-mail messages aren't behaving as you expect them to, be sure to check the order of your message rules. You might find that they are being processed in the wrong order.

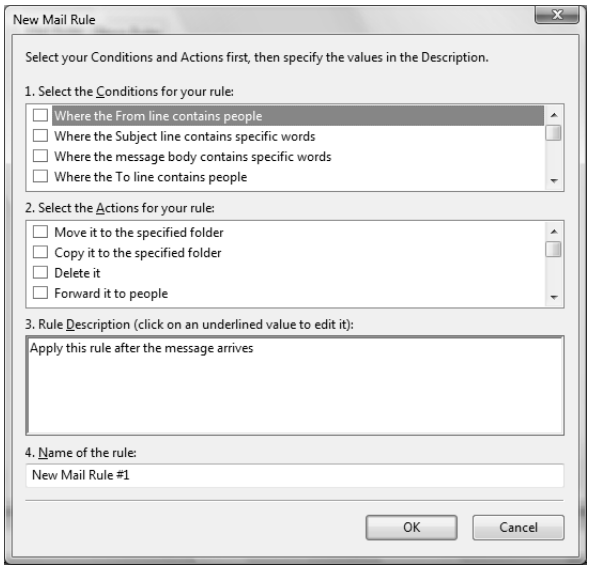
FIGURE 10.14 Message Rules dialog box



To add a message rule, click New. The New Mail Rule dialog box, shown in Figure 10.15, will appear. As you can see, there are many conditions and actions. Experiment with them to see what they can do.

In Exercise 10.3, you will create a new mail rule that will forward all e-mail messages.

FIGURE 10.15 New Mail Rule dialog box



EXERCISE 10.3

Adding a New Mail Rule

1. In Windows Mail, click Tools ➢ Message Rules ➢ Mail.
2. If the Message Rules dialog box is displayed, click New.
3. The New Mail Rule dialog box will open. Select the check box next to the condition named For All Messages.
4. Select the check box next to the action named Forward It to People.
5. In the Rule Description box, click the underlined word People.

EXERCISE 10.3 *(continued)*

6. In the Address field, type the e-mail address that should receive your forwarded messages, then click OK.
7. In the Name of the Rule box, type a name for your rule, then click OK. The rule will be created.
8. If you want to apply the rule to your existing messages, click Apply Now. On the next screen, select the rule, and click Apply Now.

Configuring Advanced Options

Clicking Tools ➢ Options will enable you to configure Windows Mail options. The General tab, shown in Figure 10.16, is used to configure general options, how messages are sent and received, and default messaging programs.

The Read tab, shown in Figure 10.17, is used to configure the behavior of Windows Mail when messages are read. It is also used for newsgroup behavior and the default font and encoding method that are used for reading messages.

The Receipts tab, shown in Figure 10.18, is used to configure whether read receipts are requested or sent. Secure receipts can also be configured.

FIGURE 10.16 Options dialog box, General tab

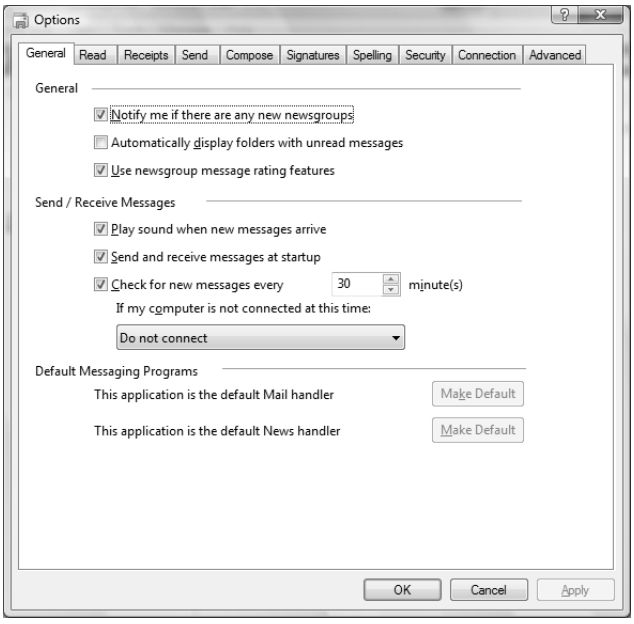


FIGURE 10.17 Options dialog box, Read tab

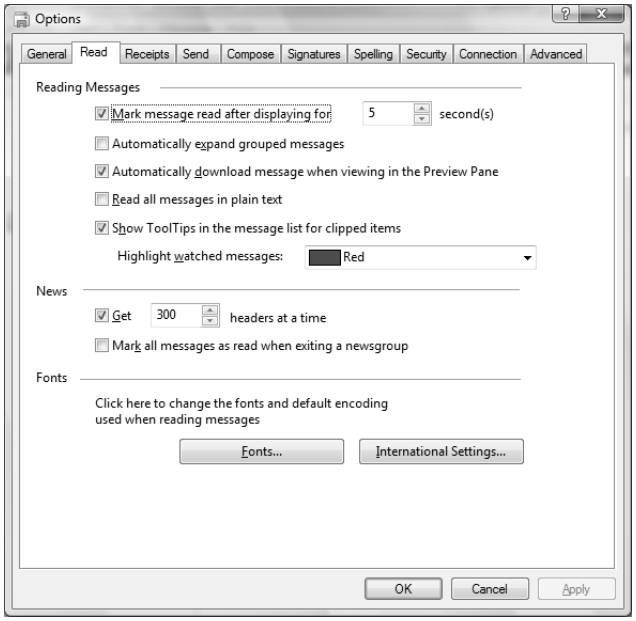
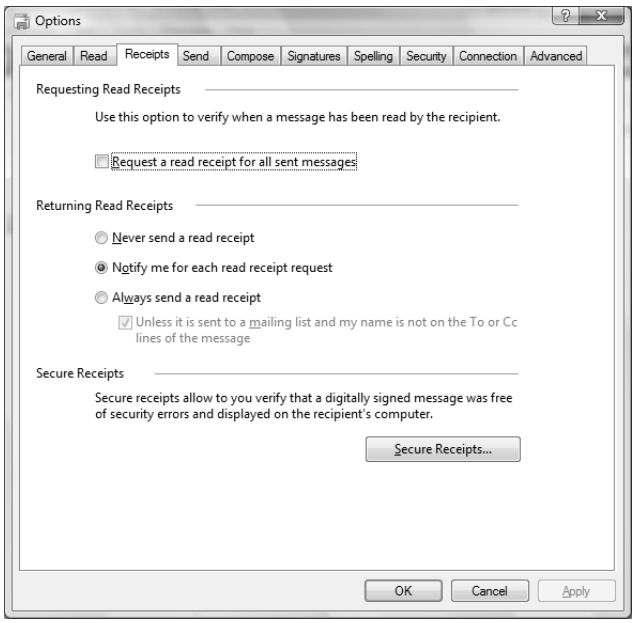


FIGURE 10.18 Options dialog box, Receipts tab



The Send tab, shown in Figure 10.19, is used to configure the behavior of Windows Mail when messages are sent. It is also used to configure whether mail and newsgroup messages are sent in HTML or plain text.

The Compose tab, shown in Figure 10.20, is used to configure the default font, stationery, and business card that are used for sending mail and newsgroup messages.

The Signatures tab, shown in Figure 10.21, is used to add, remove, and configure signatures. Signatures can be automatically added to the bottom of outgoing messages.

The Spelling tab, shown in Figure 10.22, is used to configure whether Windows Mail will check for spelling errors, whether certain words are ignored, and what language should be used.

The Security tab, shown in Figure 10.23, is used to configure virus protection features, such as whether an application attempts to send an e-mail on behalf of you. You can also configure Windows Mail to block attachments and images that could potentially be harmful. Secure Mail digital ID certificates can also be configured. Finally, you can configure encryption and signing for all outgoing messages.

FIGURE 10.19 Options dialog box, Send tab

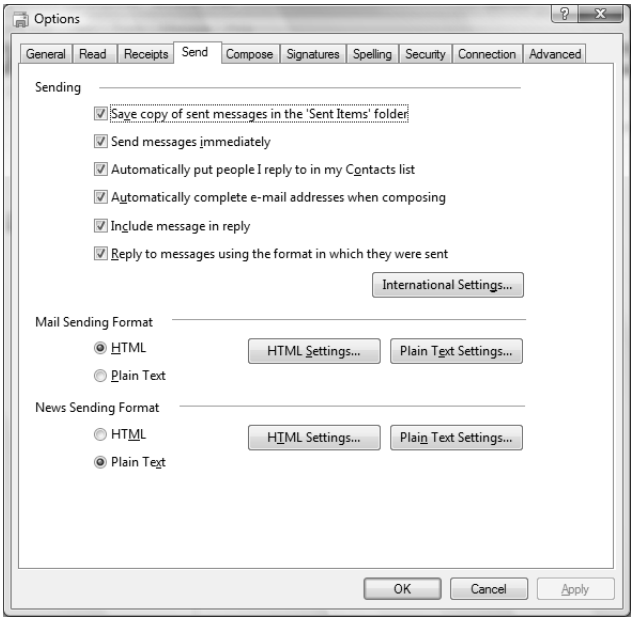


FIGURE 10.20 Options dialog box, Compose tab

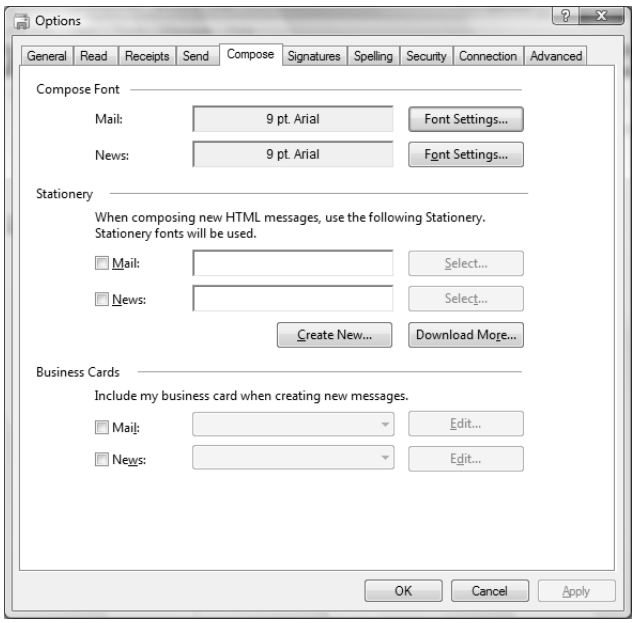


FIGURE 10.21 Options dialog box, Signatures tab

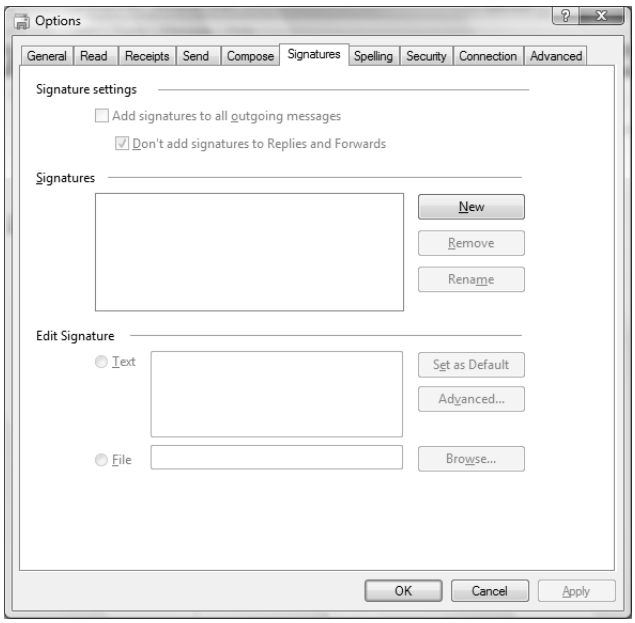


FIGURE 10.22 Options dialog box, Spelling tab

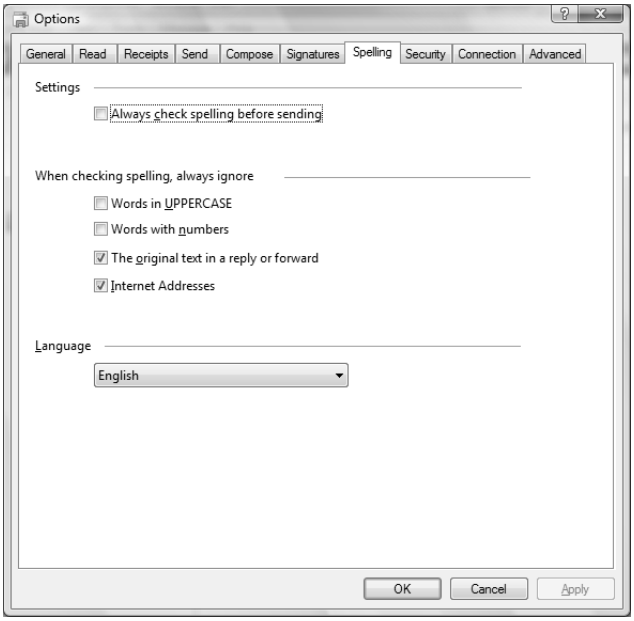
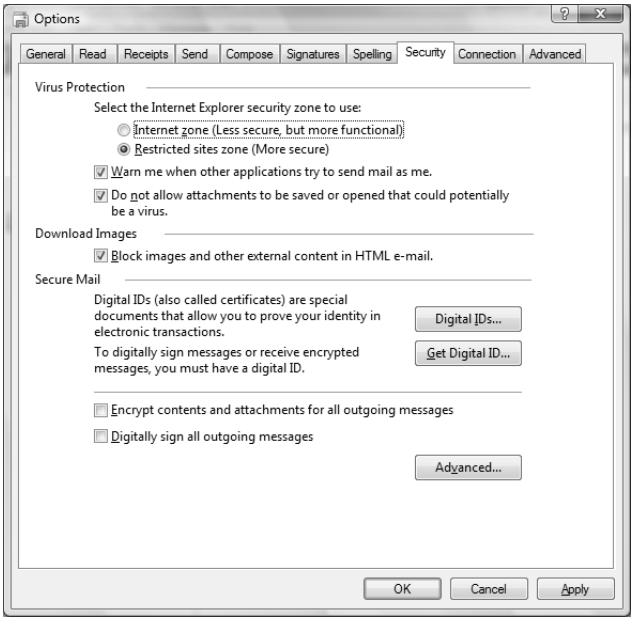


FIGURE 10.23 Options dialog box, Security tab



The Connection tab, shown in Figure 10.24, is used to configure dial-up and Internet connection behavior. Windows Mail uses the same Internet Connection settings that Internet Explorer uses.

Finally, the Advanced tab, shown in Figure 10.25, is used to configure the behavior of contacts, IMAP settings, message threads, replies, and forwards. You can also click the Maintenance button to open the dialog box shown in Figure 10.26, which lets you configure maintenance tasks, such as whether deleted items are emptied on exit and how the database is compacted.

FIGURE 10.24 Options dialog box, Connection tab

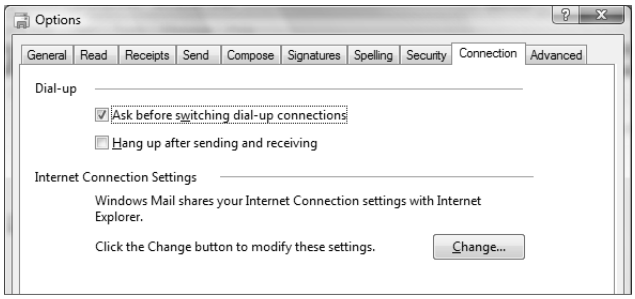


FIGURE 10.25 Options dialog box, Advanced tab

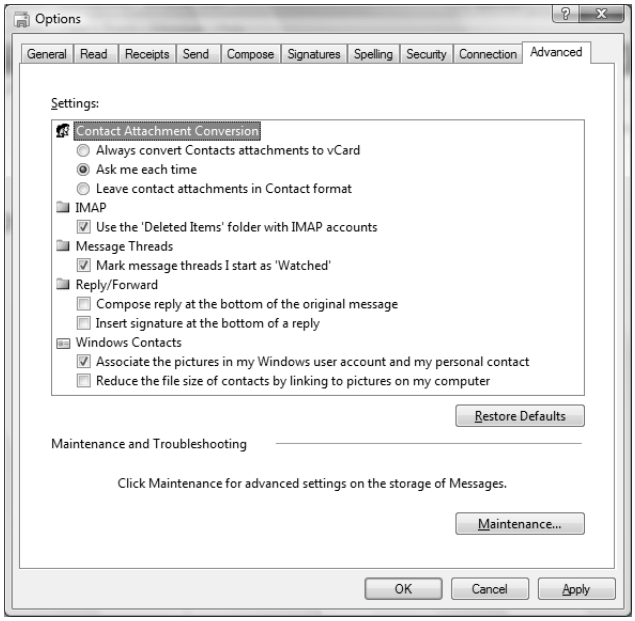
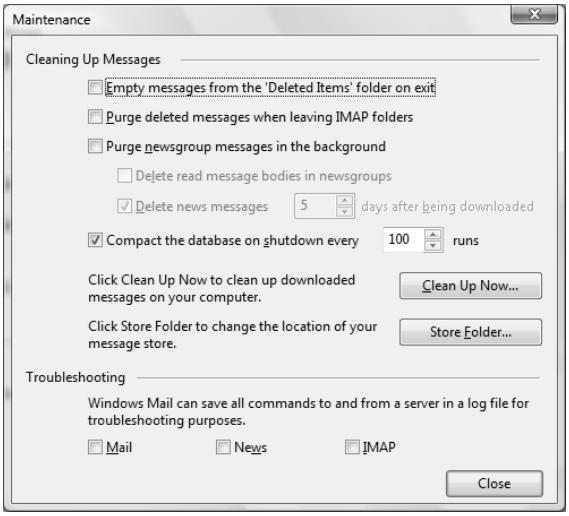


FIGURE 10.26 Maintenance dialog box



Importing and Exporting

Importing and exporting can help you to easily transfer Windows Mail data from one computer to another. You can import and export contacts, messages, mail account settings, and news account settings.

Contacts can be imported and exported using the following formats:

- Import
  - Comma Separated Values (CSV)
  - LDIF
  - vCard (VCF)
  - Windows Address Book (from Outlook Express)
- Export
  - Comma Separated Values (CSV)
  - vCard (VCF)

Messages can be imported and exported using the following formats:

- Import
  - Microsoft Exchange
  - Microsoft Outlook

- Microsoft Outlook Express 6
- Microsoft Windows Mail 7

- Export
  - Microsoft Exchange
  - Microsoft Windows Mail

Using the New Features in Windows Mail

Windows Mail contains many new and upgraded features compared with Outlook Express. Search functionality has improved, a Communities feature has been added, and security features have been enhanced.

Improved Search

Searching for e-mail messages is easier than ever with Windows Mail. Simply type a search phrase in the search box, located in the upper-right corner, and a list of messages that contain that phrase will appear. The phrase can occur anywhere in the header or message body in any message in any folder or subfolder. You can also search your e-mail messages by searching from the Windows search box.

Windows Mail Communities

Like Outlook Express, Windows Mail can be used to read e-mail and newsgroups. The Communities feature enables you to rate posts based on their usefulness. Communities uses Windows Live ID to ensure that individuals who post to newsgroups are authentic. However, you can disable that functionality. You can get help from users in the Microsoft Discussion Groups by clicking Help ➢ Questions & Answers from Communities. You can access other newsgroups by clicking Tools ➢ Newsgroups.

Windows Mail Security Features

Windows Mail includes junk e-mail and phishing filter technology to help keep your Inbox clean of unwanted e-mail messages. Microsoft SmartScreen is used to move suspected junk e-mail to the Junk E-mail folder.

Junk e-mail filters and phishing filters are both configured by clicking Tools ➢ Junk E-mail Options. The Junk E-mail Options dialog box, shown in Figure 10.27, will be displayed.

The Options tab is used to configure the level of filtering that will occur. The following levels are available:

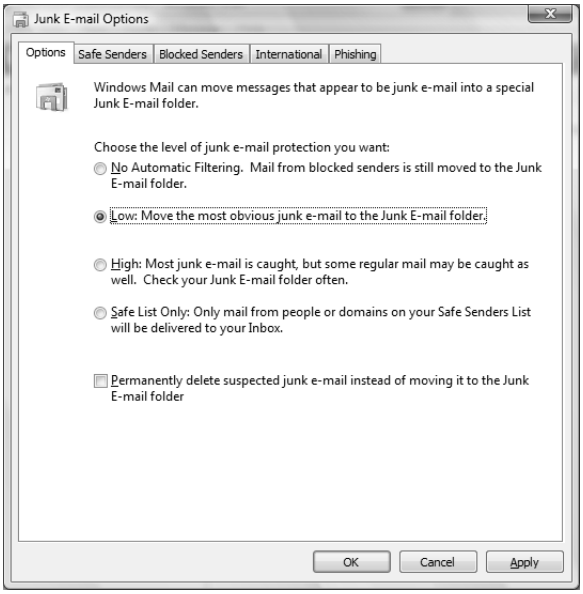
No Automatic Filtering Only messages from people and domains on the Blocked Senders list will be moved to the Junk E-mail folder.

Low Only the most obvious junk e-mail will be moved to the Junk E-mail folder.

High Most junk e-mail will be moved to the Junk E-mail folder.

Safe List Only Only messages from people and domains on the Safe Senders list will be delivered to the Inbox; all other messages will be moved to the Junk E-mail folder.

FIGURE 10.27 Junk E-mail Options, Options tab



Although the High filtering level provides a high level of junk e-mail filtering, some normal e-mail messages might also appear in the Junk E-mail folder. This is called a "false positive." You should regularly check your Junk E-mail folder to see whether some wanted e-mail was inadvertently filtered.

You can also configure Windows Mail to permanently delete messages rather than move them to the Junk E-mail folder. However, take care when using this feature with the High or Safe List Only filtering level, as you might be deleting messages that you want to receive.

The Safe Senders tab, shown in Figure 10.28, displays the e-mail addresses and domain names that are marked as safe. E-mail messages from people in your Windows Contacts can also be marked as safe. You can also configure Windows Mail to automatically add people to your Safe Senders list after you send them a message.

The Blocked Senders tab, shown in Figure 10.29, displays the e-mail addresses and domain names that should be blocked. Messages from these accounts or domains will be moved to the Junk E-mail folder (or deleted, if you have configured Windows Mail to do so).

Be sure that you do not add an e-mail address or domain name to both your Safe Senders list and your Blocked Senders list. This will cause messages from the e-mail address or domain name to be delivered to your Inbox.

FIGURE 10.28 Junk E-mail Options, Safe Senders tab

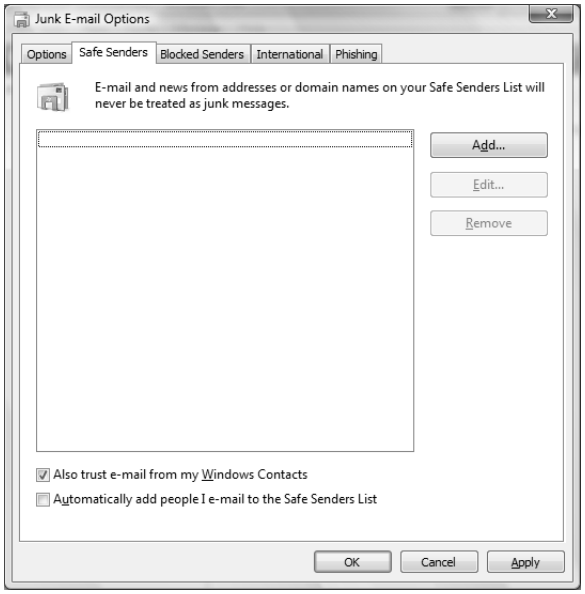
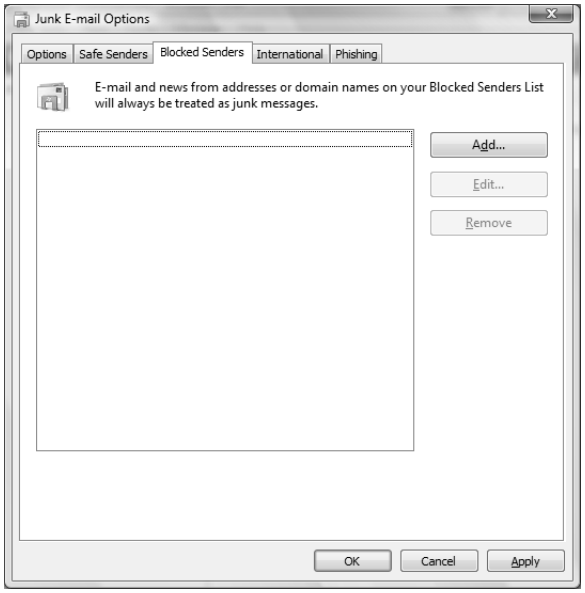


FIGURE 10.29 Junk E-mail Options, Blocked Senders tab



If a conflict arises where an e-mail address is in one list, and the corresponding domain is in the other list, the specific e-mail address takes precedence. Thus, you can block all e-mail messages from a domain except for a specific user.

The International tab, shown in Figure 10.30, can be used to block e-mail from certain top-level domain country codes. You can also block messages that use a particular encoding.

The Phishing tab, shown in Figure 10.31, is used to block *phishing* attacks. Phishing e-mails attempt to trick you into disclosing your personal or financial information, such as your online banking password or your credit card number. Windows Mail will allow you to view phishing e-mails, but will block any dangerous links or content. You can mark a message as safe if you are certain that the message is from a trusted source. You can also configure Windows Mail to automatically move suspected phishing messages to the Junk E-mail folder.

When you receive an e-mail message, you can add the sender's e-mail address or the sender's domain to the Safe Senders or Blocked Senders list. To do this, right-click the message, select Junk E-mail, and click one of the following options:

- Add Sender to Safe Senders List
- Add Sender's Domain to Safe Senders List
- Add Sender to Blocked Senders List
- Add Sender's Domain to Blocked Senders List

FIGURE 10.30 Junk E-mail Options, International tab

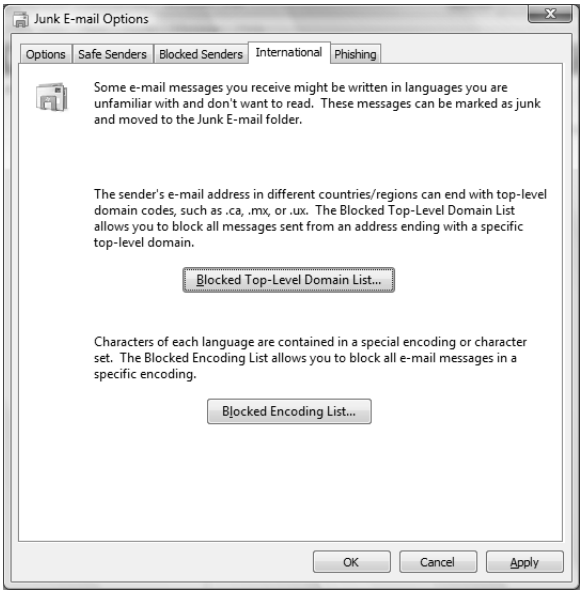
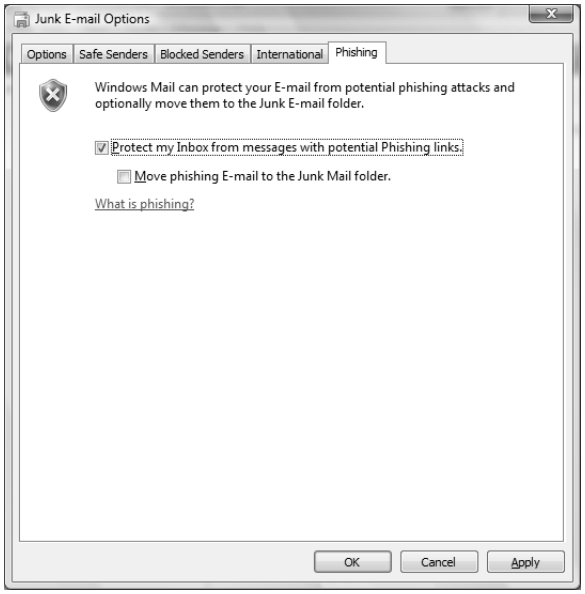


FIGURE 10.31 Junk E-mail Options, Phishing tab



Two other options are available on certain messages when you right-click and select Junk E-mail:

- Mark as Not Junk
- Unblock

Mark as Not Junk can be used on a message that was inadvertently moved to the Junk E-mail folder. Unblock can be used on a message to unblock images and links in the message.

In Exercise 10.4, you will manually add a domain name or an e-mail address to your Safe Senders list.

EXERCISE 10.4

Adding an Entry to the Safe Senders List

1. In Windows Mail, click Tools ➢ Junk E-mail Options.
2. Click the Safe Senders tab.
3. Click the Add button.
4. Type an e-mail address or domain name, then click OK.
5. Click Apply or OK.

Using Windows Contacts

Windows Contacts, shown in Figure 10.32, is a new program in Windows Vista that can be used to store contact information for individuals. Windows Contacts can be accessed from within Windows Mail by clicking Tools ➢ Windows Contacts. If Windows Mail is not open, you can access Windows Contacts by clicking Start ➢ All Programs ➢ Windows Contacts.

From here, you can create, modify, and delete contacts and contact groups. You can also use your default e-mail program to compose an e-mail message to the selected contact.

Adding a new contact is as simple as clicking the New Contact button. Within each contact, you can record a great deal of information, including the following:

- Full name
- Title
- Nickname
- E-mail address
- Home address, phone, fax, cell, and website
- Work address, phone, fax, pager, and website

FIGURE 10.32 Windows Contacts

- Gender
- Birthday
- Anniversary
- Spouse/partner name
- Children names
- Notes
- Digital IDs

Windows Contacts was designed to be used with Windows Mail or as a stand-alone program. However, third-party e-mail client applications can also use Windows Contacts as long as they can read the `.contact` files. If your e-mail client application cannot read `.contact` files, you can export the contacts from Windows Contacts to vCards or to a CSV file.

New contacts can also be added to Windows Contacts from within Windows Mail. To do so, right-click a message in Windows Mail and select Add Sender to Contacts.

Using Windows Calendar

Windows Calendar, shown in Figure 10.33, is a new program in Windows Vista that can be used to store appointments and tasks. Windows Calendar can be accessed from within Windows Mail by clicking Tools ➢ Windows Calendar. If Windows Mail is not open, you can access Windows Calendar by clicking Start ➢ All Programs ➢ Windows Calendar.

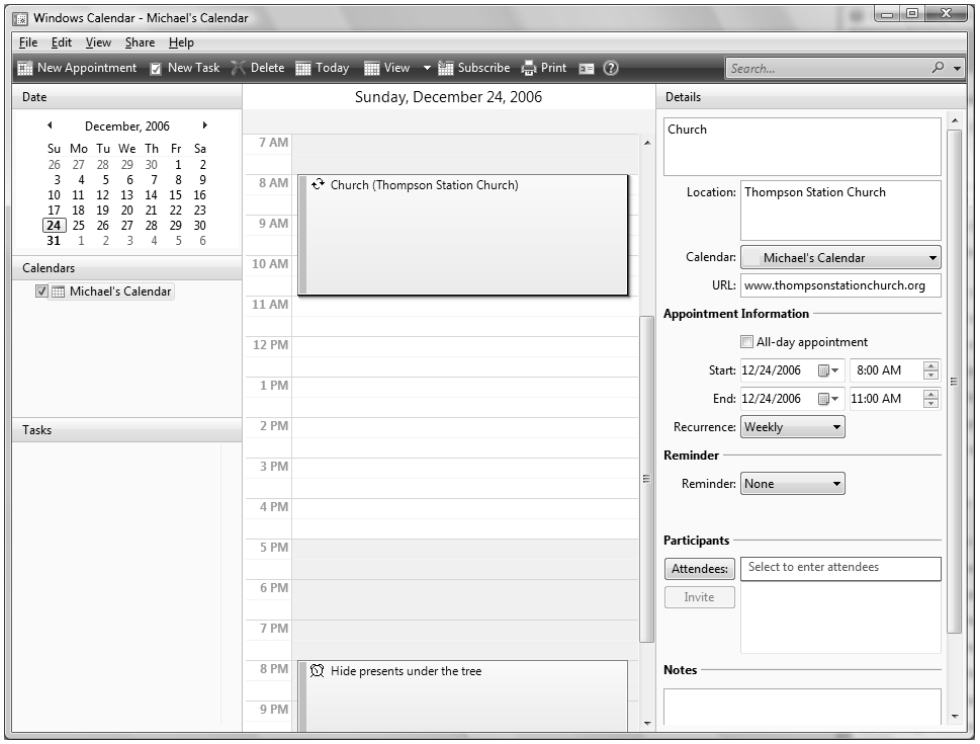
You can perform the following tasks with Windows Calendar:

- Create one-time and recurring appointments
- Add reminders for appointments
- Create tasks
- Create multiple calendars
- Invite attendees to appointments
- View calendar by day, work week, full week, or month
- Print your calendar
- Publish your calendar
- E-mail your calendar
- Subscribe to another person's calendar

To create an appointment, click the New Appointment button, then adjust the day and time. If it is an all-day event, select the All-Day Appointment check box.

If the appointment is a recurring event, select the recurrence from the drop-down list. Recurring appointments can occur daily, weekly, monthly, yearly, or at an interval you select (such as every three days). Recurring events are marked on the calendar with two circular arrows, as shown in Figure 10.33.

FIGURE 10.33 Windows Calendar



If you need a reminder, you can select the reminder time from the drop-down list. You can specify that Windows Calendar remind you of an appointment several minutes, hours, days, or weeks in advance, or you can select to be reminded on a certain date. Reminders are marked on the calendar with an alarm clock, as shown in Figure 10.33.

Clicking Today will take you to the current day. Clicking View will enable you to view the calendar by day, workweek, full week, or month. Clicking Print will enable you to print your calendar by day, workweek, full week, or month.

You can publish your calendar so others can see it. To publish a calendar, follow these steps:

1. Click Share ➤ Publish.
2. Enter the name of your calendar.
3. Enter the location where you want to publish your calendar. You can publish your calendar to the Internet, a network location, or to a shared folder on your computer so that others can view it.
4. Select whether you want to automatically publish changes you make to this calendar.

If you do not select Automatically Publish Changes Made to This Calendar, you will have to manually synchronize your calendar in order to send any changes to your published calendar location. To do so, click Share ➢ Sync.

5. Select which calendar details you want to include. You can choose to include Notes, Reminders, and Tasks.
6. Click Publish. Your calendar will be published to the selected location as an iCalendar file with an `.ics` extension.
7. Click Announce to open an e-mail message that will enable you to announce your published calendar details, or click Finish to close the Publish Calendar window.

After you have published the calendar, you can stop publishing the calendar by selecting Share ➢ Stop Publishing. To resend the announcement e-mail, select Share ➢ Send Publish E-mail.

You can also e-mail your entire calendar or an individual appointment to another person by clicking Share ➢ Send via E-mail. The calendar or appointment will be sent as an iCalendar file with an `.ics` extension.

Some organizations offer their calendars on the Internet. For example, you may want to download the schedule for your favorite hockey team. To subscribe to a calendar, click Subscribe and enter the web location of the calendar. Subscribed calendars must be in iCalendar format, which have an `.ics` filename extension.

Using Windows Fax and Scan

Windows Fax and Scan enables you to send and receive faxes without a fax machine. You can also use Windows Fax and Scan to scan documents so that you can fax or e-mail them.

To configure fax support and set fax properties, select Start ➢ All Programs ➢ Windows Fax and Scan. The Windows Fax and Scan application will start, as shown in Figure 10.34.

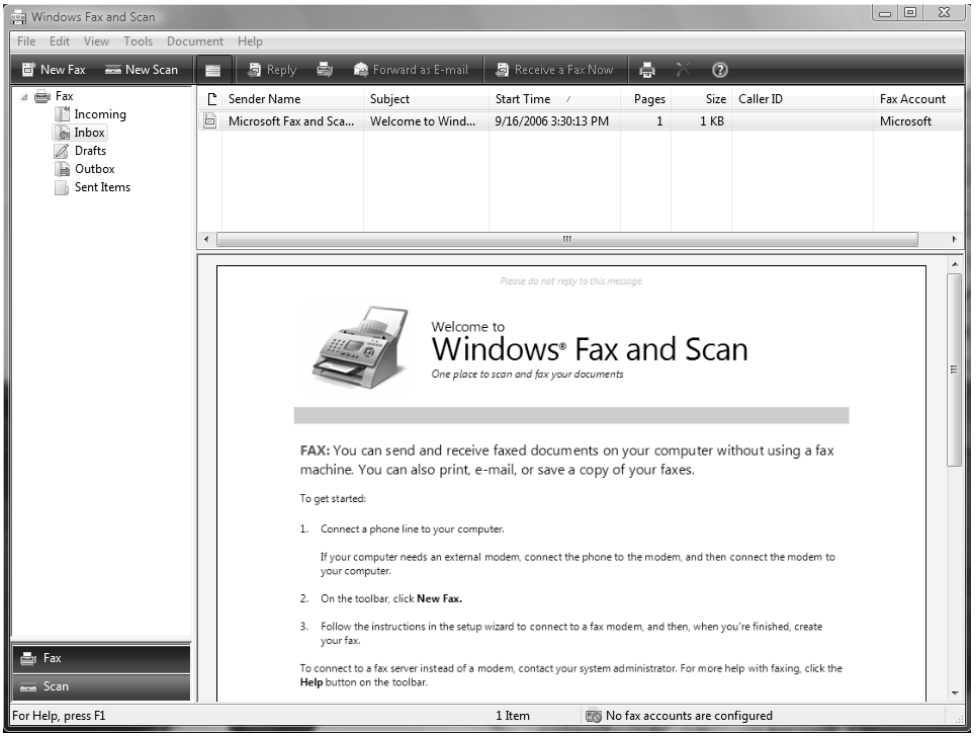
Configuring Fax Support

Windows Vista allows you to add and configure fax support. You can add fax support to your computer even if a fax machine is not available. You configure fax support through the Windows Fax and Scan application.

Adding a Fax Account

Before you can send or receive faxes, you must first create an account. To create an account, click Tools ➢ Fax Accounts, then click Add to create an account. You will be prompted to connect to a fax modem on your computer or to a fax server.

FIGURE 10.34 The Windows Fax and Scan application



If Windows Firewall is enabled, you will not be able to receive faxes until you create an exception for Windows Fax and Scan.

Setting Fax Properties

You can configure fax settings by clicking the Tools menu and selecting Fax Settings. The Fax Settings dialog box, shown in Figure 10.35, has four tabs with options and information for your fax support:

General Displays the device name and provides the ability to configure a device to send and receive faxes.

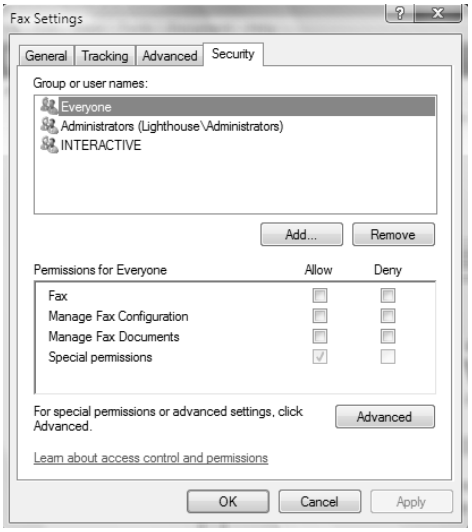
Tracking Enables you to set up notification options for fax events, and configure the Fax Monitor to display progress when faxes are sent or received.

Advanced Enables you to configure which folder is used for receiving faxes. Sent faxes will also be stored in the specified folder. Allows you to include a banner with the fax. Lets

you configure the number of redials to perform, and the start and end times for sending faxes.

Security Enables you to configure which users or groups can send and receive faxes and who can manage fax configuration.

FIGURE 10.35 The Fax Settings dialog box



Starting the Fax Service

After you configure fax support, you need to start the Fax Service in Windows Vista. To start the service, take the following steps:

1. Right-click Computer from the Start menu and select Manage from the context menu.
2. Expand Services and Applications and then Services.
3. Double-click Fax Service and click the Start button.
4. Select Automatic as the Startup Type and click OK.
5. Close the Computer Management window.

Managing Imaging Devices

A scanner is a device that can read text or graphics that are on paper and translate the information to digital data that the computer can understand. After you install a scanner on a Windows Vista computer, you can manage the device through the Windows Fax and Scan application.

If the scanner is a USB scanner, simply connecting the device to the computer should install the appropriate driver, and the scanner will be available in the Windows Fax and Scan application.

Real World Scenario

Setting Up Send and Receive Fax Support

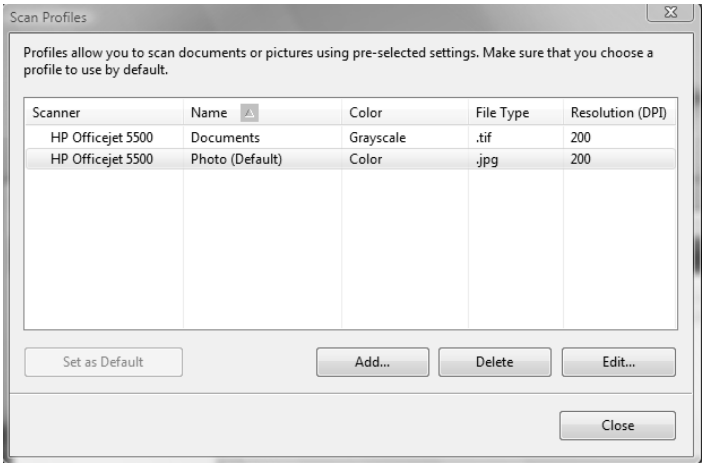
Your boss asks you to configure fax support on a computer for a user in the sales department. After you configure the fax support, the user complains that the computer will send but not receive faxes.

To enable a computer to receive faxes, you will need to do four things. First, verify that a fax account has been created by clicking Tools ➢ Fax Accounts. Second, verify that the Windows Fax and Scan application is configured to receive faxes by clicking Tools ➢ Fax Settings. Third, verify whether Windows Fax and Scan is allowed as an exception through Windows Firewall. Finally, verify that the Fax service has started. You can access Services by clicking Start ➢ Control Panel ➢ Administrative Tools ➢ Services.

In this scenario, a fax account exists because the user can send faxes. Additionally, the fax service is most likely running because the user can send faxes. The most likely reasons why the user cannot receive faxes are because Windows Fax and Scan isn't configured to receive faxes, or because Windows Firewall does not have an exception for Windows Fax and Scan.

To configure a scanner that is attached to your computer, click Scan in the lower-left corner of the Windows and Fax application, and then click Scan Settings on the Tools menu, which opens the Scan Profiles dialog box, as shown in Figure 10.36.

FIGURE 10.36 Scan Profiles dialog box



If you have a scanner installed on your computer, you can complete the steps in Exercise 10.5 to view and configure its properties.

EXERCISE 10.5

Managing and Monitoring Imaging Devices

1. Select Start ➢ All Programs ➢ Windows Fax and Scan.
2. In the Windows Fax and Scan application, click Scan in the lower-left corner.
3. Select the scanner to modify, then click the Edit button.
4. Modify the settings as desired, then click Save Profile.
5. Click Close to close the Scan Profiles dialog box.
6. Close the Windows Fax and Scan application.

Using Windows Meeting Space

Windows Meeting Space is Windows Vista's replacement for NetMeeting. With Windows Meeting Space, you can collaborate with up to 10 other Windows Vista users. The following list describes some of the things you can do with Windows Meeting Space:

- Share an application
- Show your desktop
- Distribute documents
- Collaboratively edit documents with other users
- Create notes for users

To start Windows Meeting Space, click Start ➢ All Programs ➢ Windows Meeting Space. When you launch Windows Meeting Space for the first time, you will be prompted to enable file replication and configure *People Near Me*, as shown in Figure 10.37. If you click Yes, the People Near Me dialog box will appear, as shown in Figure 10.38. You'll be asked to create a display name, configure whether you want to be signed in when Windows starts, and specify from whom you want to allow invitations. You can choose to accept invitations from Anyone, Trusted Contacts, or No One.

You can access People Near Me from Control Panel.

FIGURE 10.37 Windows Meeting Space Setup

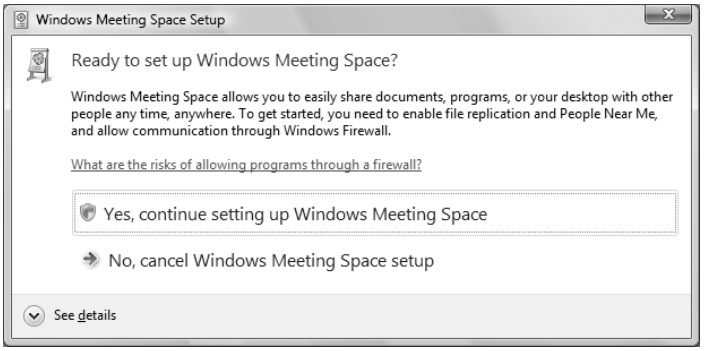
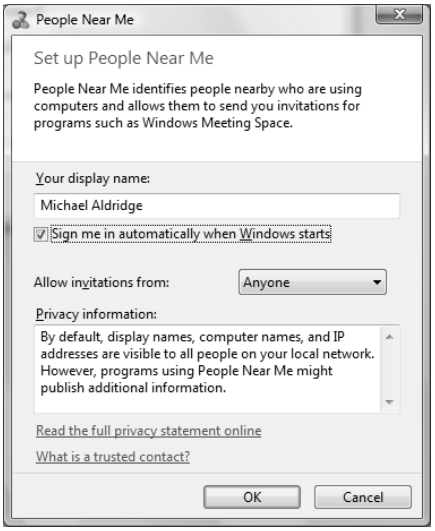


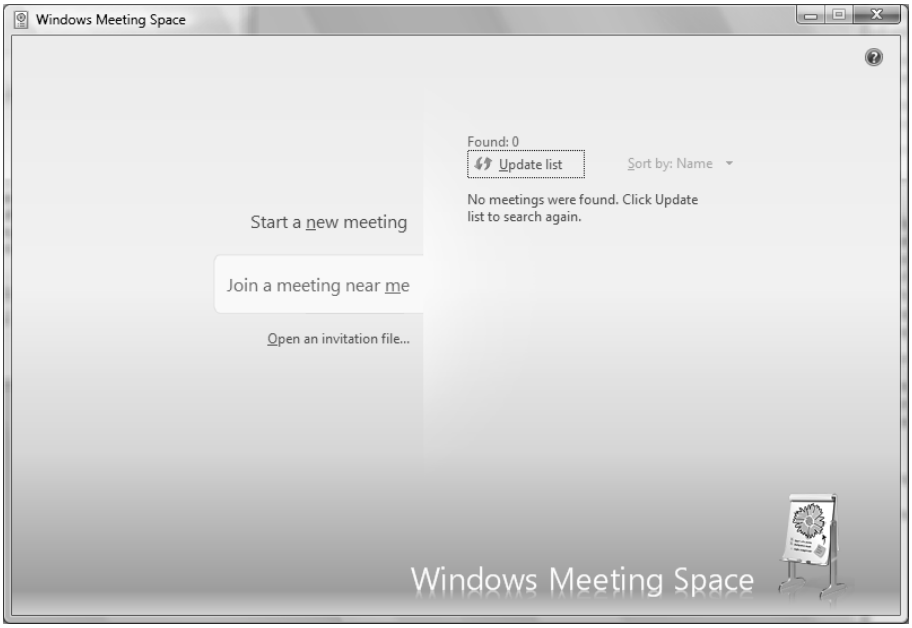
FIGURE 10.38 People Near Me



When everything is configured, Windows Meeting Space will launch, as shown in Figure 10.39. From here, you can start a new meeting, join a meeting near you, or open an invitation file.

If you have Windows Vista Home Basic, you will not be able to start a new meeting; you can only join an existing meeting.

FIGURE 10.39 Windows Meeting Space



To start a new meeting, click Start a New Meeting, then type the meeting name and a password that is at least eight characters long. You can also click Options to select whether people near you can see the meeting, or to create a private ad hoc wireless network. After you click the green arrow next to the password, the session will start, as shown in Figure 10.40. All data will be encrypted before it is sent.

The Meeting button is used to save handouts, to leave the meeting, or to exit the application. When you leave a meeting, the meeting will continue until all attendees have left the meeting.

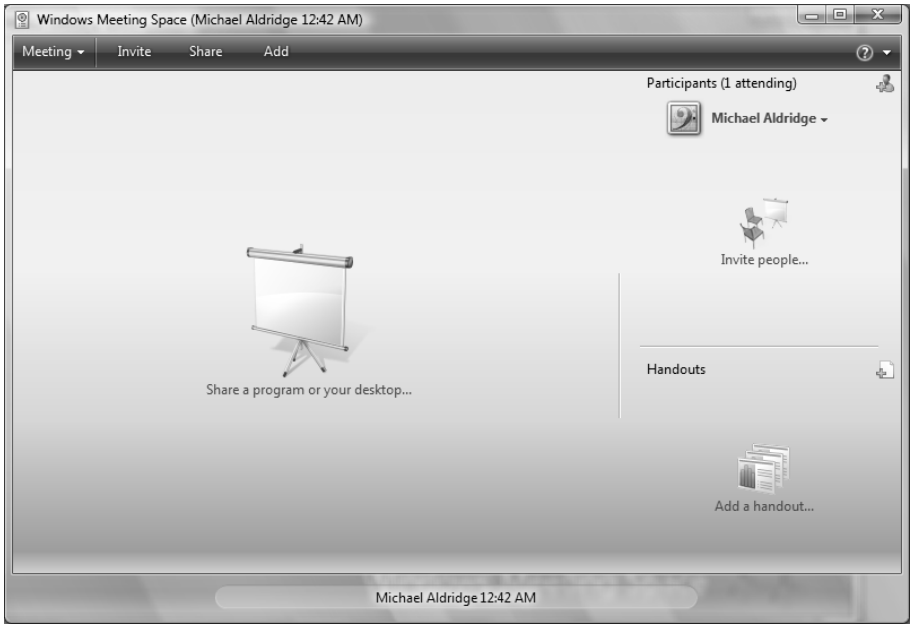
You can be in only one meeting at a time, and you can have only one instance of Windows Meeting Space running on a computer. If you are in a meeting, you must first leave the meeting in order to join or start a new one.

The Invite button is used to invite attendees. You can invite people using the following methods:

- Invite people that show up in People Near Me.
- Send an invitation via e-mail.
- Create an invitation file, which you can then share or send in an instant message.

Invitations are sent as a `.wcinv` file.

FIGURE 10.40 Windows Meeting Space, active meeting



The Share button is used to share an application or your entire Desktop. When you share an application or your Desktop, only you have control unless you explicitly give control by clicking the Give Control button. You can also actively take back control by clicking the Take Control button, or by clicking the Windows key and Esc.

The Add button is used to add documents called *handouts* in Windows Meeting Space. Only one person can edit a handout at a time, and any changes will be distributed to all users. However, changes are not saved to your original document.

Files encrypted with Encrypting File System (EFS) cannot be shared as handouts.

Troubleshooting Windows Meeting Space

Here are some steps you can take to troubleshoot Windows Meeting Space problems:

If Windows Meeting Space will not start:

- Ensure IPv6 is enabled. IPv6 is required for Windows Meeting Space.
- Ensure you are logged in using a standard or administrator user account, not a guest account.

- Ensure you can access Windows Contacts.
- Ensure you have more than 12MB of hard disk space.
- Ensure the Peer Name Resolution Protocol, Peer Networking Grouping, Peer Networking Identity Manager, and DFS Replication services are running.
- Ask your network administrator if peer-to-peer networking features have been disabled.

If you cannot not receive invitations sent through People Near Me:

- Ensure that you are signed in to People Near Me.
- Ensure that you have created an exception for Windows Meeting Space in Windows Firewall or your third-party firewall application.
- Ensure that you are on the same subnet as the other meeting participants. Users must be on the same subnet to be discovered by People Near Me.
- Ask your system administrator if People Near Me has been disabled by a Group Policy setting.

If your users cannot be seen in People Near Me, you can still invite them by e-mail or by sending them an invitation file.

If you cannot connect to a meeting:

- Ensure that you are using Windows Vista. Windows Meeting Space is compatible only with Windows Vista.
- Ensure that you have created an exception for Windows Meeting Space in Windows Firewall or your third-party firewall application.
- Ensure that you have network connectivity to the meeting.
- Ensure you are typing the correct password.
- If IPSec is used, ensure that you are using the same IPSec policy as the meeting originator.

Using Windows Media Player 11

Windows Media Player 11, shown in Figure 10.41, enables you to play digital media, organize your media files, rip music from CDs, burn CDs and DVDs, synchronize files to a portable music player, and shop for digital media online.

The following tabs are available in WMP 11:

Now Playing Used to play a CD or DVD, add enhancements, watch visualizations, and manage plug-ins.

Library Used to organize your digital media, create playlists, add files to your digital media library, and share your media. You can organize your music, pictures, video, recorded TV, or other media.

Rip Used to copy music from a CD. You can rip at various bit rates using the following formats:

- Windows Media Audio (WMA)
- MP3
- WAV (lossless)

Burn Used to burn music to a CD or data to a CD or DVD. You can burn at various speeds, apply volume leveling to audio CDs, and convert music to a different bit rate.

Sync Used to perform two-way synchronization of data between your computer and a portable media device, a flash memory device, or a Portable Media Center.

Online Stores Used to shop online for digital media. The URGE store is selected by default.

When you play, burn, or sync a protected file, Windows Media Player checks to see if you have valid media usage rights. If you have valid rights, you will be allowed to play, burn, or sync the file. Normally, media usage rights are automatically downloaded for you. So why can't you play your file if you've got a connection to the Internet? Check to see if Download Usage Rights Automatically When I Play or Sync a File is selected on the Privacy tab of the Options dialog box. If it is enabled, you might have to restore your media usage rights from the online store where you purchased your digital media.

FIGURE 10.41 Windows Media Player 11

Dealing with Digital Rights Management (DRM) in Windows Vista

You're listening to a bunch of music files on your computer. All of a sudden, your computer displays an error message, which states that you do not have rights to play the file. But you have local administrator rights on your computer! Why wouldn't you have rights to play the file? The file is probably protected by *Digital Rights Management (DRM).*

DRM is used by content providers to control how and where digital music and videos that you have purchased from them are played. These content providers are often online stores that sell these songs and videos for a one-time fee or as part of a subscription-based service. Files protected by DRM will allow you certain media usage rights, such as the right to play a file a specified number of times, the right to sync a file to portable media devices a specified number of times, or to burn a file to another medium a specified number of times. DRM cannot be removed from a protected file.

Media usage rights vary based on the type of file and the online provider who sells you the file. For example, you might purchase a song for a one-time fee, and the online provider may impose few or no restrictions. Or, you might download a song from a subscription service that allows you to play the song until your subscription expires.

Using Windows Media Center

Windows Media Center improves upon the features found in Windows XP Media Center Edition. You can use Windows Media Center to do the following:

- Record and watch TV (with a TV tuner card).
- Play audio or video from a file, CD, or DVD.
- Watch a slide show.
- Listen to the radio (with an FM tuner card).
- Burn a CD or DVD.
- Stream or download online music.
- Play online games on demand.
- Stream your digital media to a Windows Media Center Extender device.

Windows Media Center is available only in Windows Vista Home Premium and Windows Vista Ultimate.

An optional Windows Media Center remote control can be used to remotely control Windows Media Center.

Using Windows Media Center Extenders

A Windows *Media Center Extender (MCE) device* enables you to watch or record TV, watch videos, listen to music, and view pictures without being at the computer. Some devices that have MCE capabilities include

- Network-capable TVs
- Network-capable DVD players
- Xbox 360s

Real World Scenario

Troubleshooting the Setup of an MCE Device

You are attempting to configure an MCE-capable TV in your company's training room so that you can stream training videos to the device. However, the Media Center computer cannot detect the MCE device during setup. How should you troubleshoot this problem?

1. Ensure that you have copied the right Setup Key from the MCE device.
2. Ensure that your MCE device and computer are connected to the network and are on the same subnet.
3. If you are using a wireless network connection, ensure that the MCE device is in range of the access point and is configured with the correct security key.
4. Make sure that the correct ports are open in Windows Firewall or your third-party firewall. Windows Firewall should configure itself automatically. To configure your firewall settings manually, open the following ports for the local subnet:
   - TCP 554
   - UDP 1900
   - TCP and UDP 2177
   - TCP 3390
   - UDP 5004 and 5005
   - TCP 8554 to 8558
   - TCP 10244
   - TCP 50004 to 50013
   - UDP 7777 to 7781

To set up a Windows MCE device, follow these general steps:

1. Log onto your Windows Media Center computer and ensure that it is connected to the network.
2. Turn on your MCE device and ensure that it is connected to the network.
3. Write down the eight-digit Setup Key for your MCE device.
4. On the Windows Media Center computer, go to Tasks ➢ Add Extender.
5. Follow the prompts, and enter the eight-digit Setup Key that you wrote down in Step 3.
6. Continue to follow the prompts, then click Finish. The MCE service (mcx2svc) will start, and Windows Firewall will automatically be configured to allow MCE communications. Your MCE device is now ready to use.

You will not be expected to memorize all of the port numbers on the previous page for the exam. We merely provide them for your reference.

When using an MCE device, your Media Center computer must be turned on. If the Media Center computer goes to sleep or hibernates, or if the network card is turned off to save power, the MCE device will not be able to connect. To ensure that your Media Center computer doesn't inadvertently power down or go to sleep, modify the Power Options in Control Panel. You can also ensure that your network card doesn't shut down to save power by using the network card's software, or by modifying the device properties in Device Manager.

Using Windows SideShow

Windows SideShow enables you to view information from your computer by using an alternative display device. These devices can be integrated into your computer, such as a small LCD display on the lid of a laptop or a keyboard, or they can be separate from your computer, such as a mobile phone or a SideShow-enabled TV or LCD. To launch SideShow, click Start ➢ Control Panel ➢ Programs ➢ Windows SideShow.

To display information on a SideShow device, you must first install SideShow gadgets on your computer and associate them with the device. These gadgets can enable you to view your e-mail messages, contacts, calendar, pictures, and more. Gadgets are displayed on your device in the order you install them. You can change the order by clicking Change The Order In Which Gadgets Appear and moving the most frequently used gadgets to the top of the list.

If you have difficulty connecting your external SideShow device to your computer, ensure that your network, wireless, Bluetooth, or USB cable connection is working properly. For integrated devices, you should ensure that the device hasn't been removed from Device Manager.

Using Windows Sync Center

Windows Sync Center can be used to synchronize music and files between your computer and a network folder or mobile device. You must set up a sync partnership with a device before you can synchronize data to it. After a partnership has been established, you can synchronize manually, on a schedule, or when an event occurs, such as when you log on or log off.

You cannot synchronize with network folders using Windows Vista Starter, Windows Vista Home Basic, or Windows Vista Home Premium.

When synchronizing, the files on your computer are compared with the files on the network or device. Files that have been modified will overwrite corresponding files on the other device or network location. If a file has been modified in both locations, a sync conflict will occur, and you must choose which version to keep. If a file has been added or deleted in one location since the last sync, Sync Center will add or delete the file from the other location.

You can choose to perform one-way or two-way synchronization. With one-way synchronization, files are modified only on one device or location; no changes are made to the original file location.

Using Windows CardSpace

Windows CardSpace is new to Windows Vista. It enables you to create cards that can be used to send personal information to websites. You can perform the following actions with Windows CardSpace:

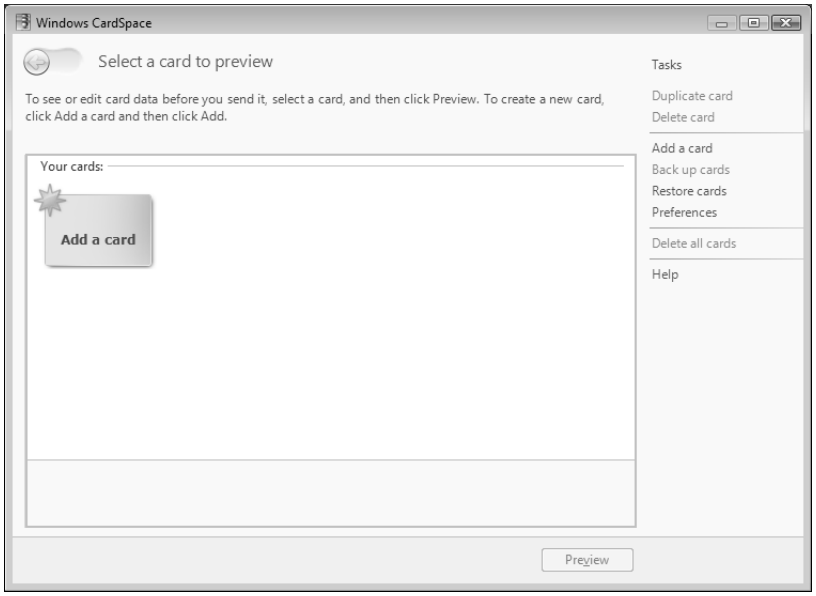
- Confirm the identity of a website that requests information from you.
- Send information to a website that requests information from you.
- Manage and review your card information before you send it to a website.

To launch Windows CardSpace, click Start ➢ Control Panel ➢ User Accounts and Family Safety ➢ Windows CardSpace. The first time you launch it, an intro screen will appear describing Windows CardSpace. After you click OK, the Windows CardSpace screen will appear, as shown in Figure 10.42.

Windows CardSpace has options to add, duplicate, back up, restore, and delete cards. Two types of cards are available:

- Personal cards are created by you and are used to send your personal data to websites quickly and easily. These cards can store your name, e-mail address, mailing address, phone numbers, birthday, gender, and website address.

FIGURE 10.42 Windows CardSpace



- Managed cards are created by online businesses and store data that they provide. For example, a bank might give you a managed card with digital credit card information, or an online service provider might issue you a digital membership card. You cannot create a managed card. Rather, it is sent to you by a managed card provider as a `.crd` file that you must install. Confidential managed card data is kept at the managed card provider's site.

Cards are not unique to a single website. You can send the same card to many different sites if the information they require is the same.

To create a personal card, follow these steps:

1. Click Add a Card on the right-hand pane. You will be prompted to select the type of card you want to add, shown in Figure 10.43.
2. Click Create a Personal Card. You will be prompted to fill in your card data, as shown in Figure 10.44.
3. Type a card name and fill in the personal information that you want to send to websites. You can also choose a picture to send. Click Save to continue. The card will be added to Windows CardSpace.

To install a managed card, you must have a `.crd` file that is issued by the managed card provider.

FIGURE 10.43 Adding a card

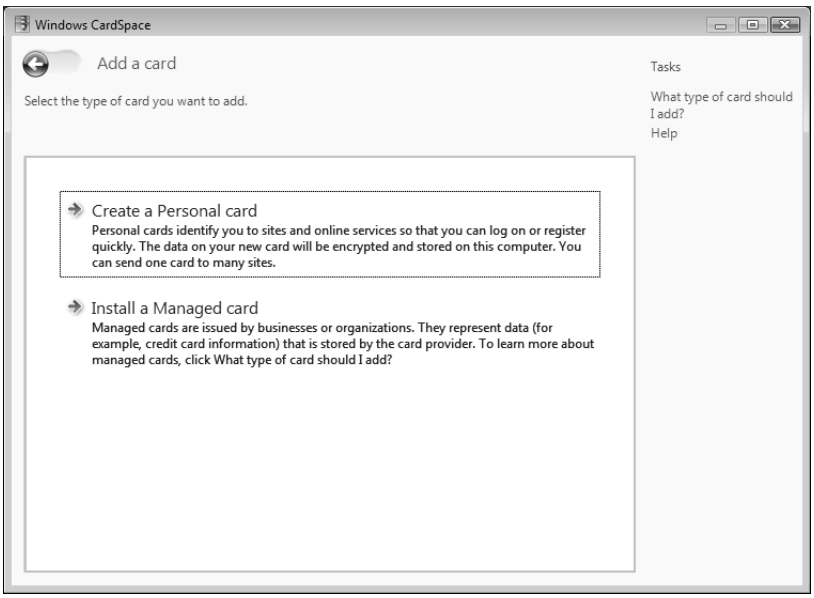
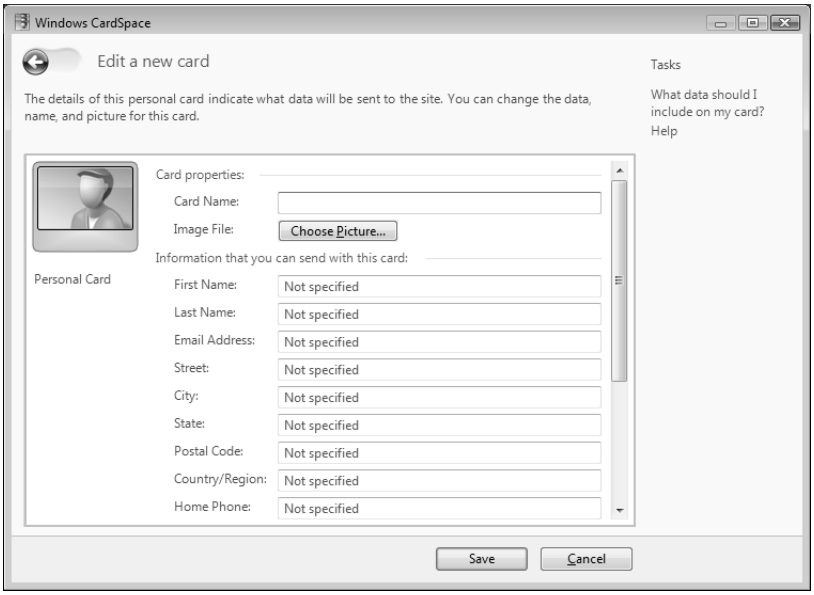


FIGURE 10.44 Entering card information



To edit a card, double-click the card, or select the card and click Preview. The Card Details screen enables you to view your card information. You can also view your card history and lock your card with a PIN. Click Edit Card in the right pane or Edit at the bottom of the window to edit the card information. After you have finished making changes, click Save.

To delete a card, select the card and click Delete Card, then confirm your action. To delete all your cards, click Delete All Cards and confirm your action. Once a card is deleted, it is permanently gone, along with its history data, and it cannot be retrieved unless you have previously saved it to a backup file.

CardSpace backups can consist of one or more cards. The card information is saved in an encrypted `.crd` backup file. If you lose your cards, or need to restore them to another computer, you can restore the `.crd` backup file using Windows CardSpace.

In Exercise 10.6, we will create a personal card.

EXERCISE 10.6

Creating a Personal Card

1. Click Start ➢ Control Panel ➢ User Accounts and Family Safety ➢ Windows CardSpace.
2. Click Add a Card.
3. Click Create a Personal Card.
4. Give the card a name and enter the information that you want to send to websites, then click Save.

Securing Your CardSpace Data

Windows CardSpace enables you to back up and restore your card data so that your information will not be lost. Card information that is stored on your computer is encrypted. Microsoft will not gain access to your card data unless you use a CardSpace card to authenticate to a Microsoft website or online service.

To further protect your cards, you should take the following actions:

- Lock your Windows Desktop when you are not sitting in front of your computer. Configure a screen saver to activate when you are idle for a number of minutes, and require password authentication to unlock the Desktop.
- Protect your CardSpace cards with a PIN number. PINs are not limited to numbers; you can use uppercase and lowercase letters, numbers, symbols, and spaces. In this way, a CardSpace PIN is more like a password than a credit card PIN. Cards that are protected with a PIN cannot be viewed, edited, or sent to a website without the PIN.

PINs must be at least four characters long, but a minimum of eight characters is recommended.

If you forget your PIN, you will probably have to delete the card and create or install a new one.

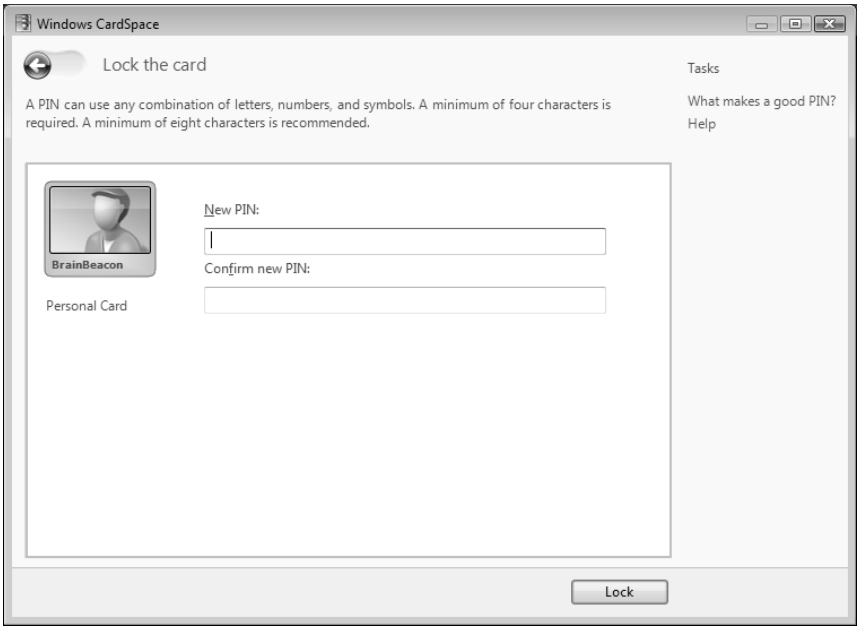
After you create a PIN to lock a card, you can remove or change the PIN from the Card Details screen. However, to do so, you must first type the current PIN to authenticate.

In Exercise 10.7, we will lock our newly created personal card with a PIN.

EXERCISE 10.7

Securing a Personal Card

1. Click Start ➢ Control Panel ➢ User Accounts and Family Safety ➢ Windows CardSpace.
2. Double-click the card you want to edit. The Card Details screen will appear.
3. Click Lock Card. The Lock the Card dialog box will appear, as shown here.



4. Enter a PIN and confirm the PIN you entered. The PIN must be at least four characters long. Then, click Lock. Your card will now be locked with your PIN.

Summary

This chapter described how to configure and use applications that come with Windows Vista. We covered the following topics:

- Using the Welcome Center
- Configuring and using Windows Sidebar
- Configuring and using Windows Mail
- Configuring and using Windows Contacts
- Configuring and using Windows Calendar
- Configuring and using Windows Fax and Scan
- Configuring and using Windows Meeting Space
- Using Windows Media Player 11
- Configuring and using Windows Media Center and Media Center Extender devices
- Using Windows SideShow
- Using Windows Sync Center
- Using Windows CardSpace

Exam Essentials

Be able to configure and troubleshoot Windows Sidebar. Know how to configure the Sidebar and gadgets.

Be able to configure and troubleshoot Windows Mail. Know how to add accounts, create message rules, import and export data, configure advanced options, and configure the junk e-mail and phishing filters.

Be able to configure Windows Calendar. Be familiar with the features of Windows Calendar. Know how to publish and subscribe to a calendar.

Be able to configure and troubleshoot Windows Fax and Scan. Know how to create an account. Be able to troubleshoot fax problems.

Be able to configure and troubleshoot Windows Meeting Space. Know how to start, join, and leave a meeting. Know the purpose of an invitation file. Be familiar with the functionality of Windows Meeting Space.

Be able to configure and troubleshoot media applications. Be familiar with the functionality of Windows Media Player 11 and Windows Media Center. Know how to set up and troubleshoot a Media Center Extender device.

Review Questions

1. You install Windows Vista on your office computer. When you log in, the Welcome Center appears. You want to stop this application from launching when you log in to Windows Vista. What should you do?
   - **A.** Remove Welcome Center from the Start ➢ All Programs ➢ Startup folder.
   - **B.** Launch the System Configuration Utility, `msconfig.exe`, and remove Welcome Center from the Startup tab.
   - **C.** Uncheck the Run at Startup check box in Welcome Center.
   - **D.** Nothing; you cannot prevent Welcome Center from launching when you log in to Windows Vista.

2. You have used Windows XP Professional for many years, and have become very familiar with the applications and administration tools that are installed with Windows XP. When you upgrade your computer to Windows Vista, you discover that many applications have been removed or replaced. Which of the following applications is still available in Windows Vista?
   - **A.** Telnet
   - **B.** HyperTerminal
   - **C.** Outlook Express
   - **D.** NetMeeting

3. A coworker has added all of the default gadgets to her Sidebar. However, only seven of them are displayed. She asks you for advice. What should you tell her?
   - **A.** Tell her that she needs to adjust the size of her Sidebar.
   - **B.** Tell her that she can see the other gadgets by clicking the left and right arrows at the top of the Sidebar.
   - **C.** Tell her that she needs to right-click the Sidebar and select Bring Gadgets to Front.
   - **D.** Tell her that she can only have a total of seven gadgets on the Sidebar.

4. You are configuring Windows Mail to be used with several e-mail accounts. When setting up the accounts, you find that only certain protocols are allowed for inbound mail. Which protocols can be used to receive inbound mail using Windows Mail?
   - **A.** HTTP
   - **B.** IMAP
   - **C.** POP3
   - **D.** SMTP

5. You are the administrator for a healthcare company. Patient confidentiality is a huge concern, so you have been asked to implement the highest level of encryption available. All of the users in your company use Windows Vista with Windows Mail. What encryption algorithm should you use?

   A. AES

   B. DES

   C. RC2

   D. 3DES

6. Your home computer network is protected by a firewall. You have configured your Windows Vista home computer to use Windows Mail. After you configure your e-mail accounts, you discover that incoming mail is not being allowed. Your e-mail provider uses POP3 and SMTP. What port should you open on the firewall?

   A. 25

   B. 110

   C. 143

   D. 995

7. One of your users has created multiple message rules. He tells you that messages from `barry@BrainBeacon.com` should be delivered to his `Barry` subfolder, but they are going to the `BrainBeacon` folder instead. What should he do to fix his problem?

   A. He should increase the rule's priority by moving it up the list.

   B. He should delete the rule and re-create it.

   C. He should fix the rule so that it delivers Barry's messages to the `Barry` folder instead of the `BrainBeacon` folder.

   D. He should add another rule to move Barry's messages from the `BrainBeacon` folder back to the `Barry` folder.

8. You have a Windows Vista computer, and you use Windows Mail for e-mail. Your computer has become outdated, and you have to export your e-mail messages and contacts. When you attempt to export your messages, what formats can you use?

   A. Microsoft Exchange

   B. Microsoft Outlook Express 6

   C. Microsoft Windows Mail

   D. Comma Separated Values

9. Your company uses Windows Mail for its messaging solution. You have been getting multiple e-mail advertisements from a company, so you add their domain to the Blocked Senders list. However, you still want to receive messages from an employee named Karen who works at that company, so you add her e-mail address to the Safe Senders list. What will happen when Karen sends you an e-mail?

   A. Her message will be delivered to the Junk E-mail folder.

   B. Her message will be delivered to the Deleted Items folder.

   C. Her message will be delivered to your Inbox.

   D. Her message will be permanently deleted.

10. You use Windows Mail to send and receive e-mail. Ever since your e-mail address was inadvertently posted to a technical forum, you have been receiving a lot of junk e-mail. You want to configure Windows Mail so that certain messages are blocked. What methods can you use to block e-mails using Windows Mail?

    A. By domain name

    B. By IP address

    C. By country code

    D. By encoding type

11. You are the commissioner of a fantasy football league. You have created a calendar in Windows Calendar that contains important dates for your league's team owners. The team owners have all sent you their e-mail addresses, so you click Share ➢ Send via E-mail to send the calendar to them. What file extension will the published calendar have?

    A. `.cal`

    B. `.ics`

    C. `.ical`

    D. `.wc`

12. You work in the records office of a university. Students regularly ask the records office to fax their official transcript to prospective employers. Windows Vista is installed on your computer, so you decide to fax the transcripts using Windows Fax and Scan. You do not have a fax account configured on Windows Fax and Scan. Your computer contains a fax modem and it is already configured. Windows Firewall is configured with an exception for Windows Fax and Scan. Which of the following statements is correct?

    A. You will be able to send and receive faxes.

    B. You will be able to send but not receive faxes.

    C. You will be able to receive but not send faxes.

    D. You will be able to neither send nor receive faxes.

13. You are the secretary for your homeowner's association. As such, you are responsible for organizing online meetings using Windows Meeting Space. You discover that you are unable to start the meeting using your Windows Vista Home Basic computer. What is the most likely reason for the problem?

A. Windows Vista Home Basic does not allow you to start a meeting.

B. You do not have an exception created for Windows Meeting Space in Windows Firewall.

C. You are already connected to a meeting, and Windows Vista Home Basic only allows you to connect to one meeting at a time.

D. Your network connection is malfunctioning.

14. You are configuring People Near Me on your Windows Vista Business computer so that you can use Windows Meeting Space with other employees on your network. After you enter your display name and configure People Near Me to sign you in when Windows starts, you must specify from whom you will receive invitations. Which of the following invitation options is not available in People Near Me?

A. Anyone

B. No One

C. Domain Users

D. Trusted Contacts

15. You are moderating a Windows Meeting Space session where you are sharing your desktop. One of the users asks to take control of the session. You click the Give Control button and the user takes control. How can you immediately reclaim control of the session?

A. Press the Windows key and Esc.

B. Click the Reclaim Control button.

C. Ask the user to click their Give Control button.

D. You cannot reclaim control of the session.

16. You are moderating a Windows Meeting Space session. A handout has been distributed to the participants. The participants ask you if they can edit the handout. How many participants can edit the handout simultaneously?

A. Only the moderator can edit the handout.

B. Only one participant at a time can edit the handout.

C. All participants can edit the handout simultaneously.

D. No participants can edit the handout after it has been distributed.

17. You have a Media Center Extender device in your living room. When you attempt to watch recorded TV, you cannot connect to the Media Center computer. Everything was working fine a few hours ago when you were watching a movie. What is the most likely problem?

A. Your Media Center computer has gone to sleep.

B. Your installation has become corrupted.

C. Your Setup Key has changed.

D. Windows Firewall is preventing access.

18. You have a computer with Windows Vista Home Premium installed. Your financial data is contained within your Documents folder. Because this data is important to you, you want to synchronize it with multiple locations. To which location or device will you not be able to synchronize your data?

A. PDA

B. SD card

C. USB flash drive

D. Network folder

19. You use Windows CardSpace to manage the information you provide to websites. Because security is important to you, you decide to lock your cards with a PIN. Which of the following are valid PINs?

A. 456

B. PredsFan#29

C. 902334

D. I am certified!

20. You have upgraded your Windows XP computer to Windows Vista. Because you do a lot of research online, you decide to use Windows CardSpace to manage the information you provide to websites. Which of the following cards can you create?

A. Managed cards

B. Payment cards

C. Personal cards

D. Trusted cards

Answers to Review Questions

1. C. To stop Welcome Center from launching when you log in to Windows Vista, you should uncheck the Run at Startup check box in Welcome Center. Welcome Center is not found in the Startup folder, and it cannot be disabled from the Startup tab of the System Configuration Utility.

2. A. Although Telnet is not enabled by default, it is still available in Windows Vista. To enable it, click Start ➢ Control Panel ➢ Programs ➢ Turn Windows Features On or Off, then select Telnet Client.

3. B. You should tell her that she can see the other gadgets by clicking the left and right arrows at the top of the Sidebar. An unlimited number of gadgets can be added to the Sidebar.

4. B, C. Windows Mail supports the use of Internet Message Access Protocol (IMAP or IMAP4) and Post Office Protocol 3 (POP3) for incoming mail. Hypertext Transfer Protocol (HTTP) message delivery is not supported in Windows Mail. Simple Mail Transfer Protocol (SMTP) is used for outgoing mail.

5. D. Triple Data Encryption Standard (3DES) should be used. 3DES uses 168-bit encryption. Although Advanced Encryption Standard (AES) uses 256-bit encryption, AES is not supported by Windows Mail.

6. B. Port 110 should be opened on the firewall. POP3, which is used for receiving inbound mail, uses port 110. SMTP is used for outbound mail and uses port 25.

7. A. He should increase the rule's priority by moving it up the list. Message rules are processed in a certain order. Rules that are ordered higher in the list will be processed first. Most likely, a rule with a higher priority is moving Barry's messages to the `BrainBeacon` folder.

8. A, C. Windows Mail can export e-mail messages to Microsoft Exchange or Microsoft Windows Mail. Messages can be imported to Windows Mail from Microsoft Exchange, Microsoft Outlook, Microsoft Outlook Express 6, and Microsoft Windows Mail 7.

9. C. Karen's message will be delivered to your Inbox. Other messages from her company's domain name will be delivered to the Junk E-mail folder unless you have configured Windows Mail to delete junk e-mail. When a conflict arises where an e-mail address is in one list, and the corresponding domain is in the other list, the specific e-mail address takes precedence.

10. A, C, D. In addition to blocking e-mail messages by e-mail address, you can configure Windows Mail to block e-mail messages by domain name, country code, and encoding type. It is not possible to block e-mail messages by IP address.

11. B. The published calendar will have an `.ics` file extension. Files with an `.ics` extension are in iCalendar format and can only be viewed by applications that support this format.

12. D. You will be able to neither send nor receive faxes. You must first have a fax account before you can send or receive faxes.

13. A. Windows Vista Home Basic does not allow you to start a meeting. You can only join an existing meeting with Windows Vista Home Basic.

14. C. You cannot configure People Near Me to accept invitations from Domain Users. Invitations can be accepted from Anyone, Trusted Contacts, or No One.

15. A. You can press Windows+Esc to reclaim control of the session. Alternatively, you can click the Take Control button to reclaim control of the session.

16. B. Only one participant at a time can edit the handout. Changes will be distributed to all participants.

17. A. Your Media Center computer has probably gone to sleep or has been turned off. Since you just watched a movie a few hours ago, it is unlikely that your Setup Key or firewall configuration has changed or that your installation has become corrupted.

18. D. You will not be able to synchronize your data to a network folder. You cannot synchronize with network folders using Windows Vista Starter, Windows Vista Home Basic, or Windows Vista Home Premium.

19. B, C, D. PredsFan, 902334, and I am certified! are valid PINs. PINs must be at least four characters long and can consist of uppercase and lowercase letters, numbers, symbols, and spaces.

20. C. You can create only personal cards. Managed cards are created by the provider as a `.crd` file that you must install.

Chapter

11

Maintaining and Optimizing Windows Vista

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Maintaining and Optimizing Systems that Run Windows Vista**
  - Troubleshoot performance issues
  - Troubleshoot reliability Issues by using built-in diagnostic tools
  - Configure data protection

To have an optimized system, you must monitor its performance. Windows Vista comes with many tools to track memory, processor activity, the disk subsystem, the network subsystem, and other computer subsystems.

In this chapter, you will learn how to monitor, maintain, troubleshoot, and optimize Windows Vista using the following utilities: Reliability and Performance Monitor, Memory Diagnostics Tool, System Information, Task Manager, Performance Information and Tools, System Tool, System Configuration, Task Scheduler, Event Viewer, Indexing Options, Remote Desktop, and Remote Assistance.

You will also learn about system recovery and troubleshooting. System recovery is the process of making your computer work again in the event of failure. In this chapter, you will learn how to safeguard your computer and how to recover from a disaster. The benefit of having a disaster recovery plan is that when you expect the worst to happen and are prepared for it, you can easily recover from most system failures.

Windows Vista contains the following recovery tools:

- Advanced Boot Options menu, including Safe Mode
- Startup Repair Tool
- Backup and Restore Center
- System Restore

We will cover all of these tools in this chapter.

Overview of System Monitoring Tools

Before you can optimize the performance of Windows Vista, you must monitor critical subsystems to determine how your system is currently performing and what (if anything) is causing system bottlenecks. Windows Vista ships with many tools that you can use to monitor system performance. Each of these utilities is covered in greater detail in this chapter. In addition, we will show you how to install and configure each utility for performance monitoring and diagnostics.

The monitoring tools allow you to assess your server's current health and determine what it requires to improve its present condition. With Reliability and Performance Monitor, you can perform the following tasks:

- Create baselines
- Identify system bottlenecks

- Determine trends
- Test configuration changes or tuning efforts
- Create alert thresholds

Each of these tasks is discussed in the following sections.

Creating Baselines

A *baseline* is a snapshot of how your system is currently performing. Suppose that your computer's hardware has not changed over the last six months, but the computer seems to be performing more slowly now than it did six months ago. If you have been using the Reliability and Performance Monitor utility and taking baseline logs, as well as noting the changes in your workload, you can more easily determine what resources are causing the system to slow down.

You should create baselines at the following times:

- When the system is first configured, without any load
- At regular intervals of typical usage
- Whenever any changes are made to the system's hardware or software configuration

Baselines are particularly useful for determining the effect of changes that you make to your computer. For example, if you are adding more memory to your computer, you should take baselines before and after you install the memory to determine the effect of the change. Along with hardware changes, system configuration modifications also can affect your computer's performance, so you should create baselines before and after you make any changes to your Windows Vista configuration.

For the most part, Windows Vista is a self-tuning operating system. If you decide to tweak the operating system, you should take baselines before and after each change. If you do not notice a performance gain after the tweak, you should consider returning the computer to its original configuration, because some tweaks may cause more problems than they solve.

Identifying System Bottlenecks

A *bottleneck* is a system resource that is inefficient compared with the rest of the computer system as a whole. The bottleneck can cause the rest of the system to run slowly.

You need to pinpoint the cause of a bottleneck to correct it. Consider a system that has a Pentium 4 3.0GHz processor with 1024MB of RAM. If your applications are memory-intensive and lack of memory is your bottleneck, then upgrading your processor will not eliminate the bottleneck.

By using Reliability and Performance Monitor, you can measure the performance of the various parts of your system, which allows you to identify system bottlenecks in a scientific manner. You will learn how to set counters to monitor your network and spot bottlenecks in the "Using Reliability and Performance Monitor" section later in this chapter.

Determining Trends

Many of us tend to manage situations reactively instead of proactively. With reactive management, you focus on a problem when it occurs. With proactive management, you take steps to avoid the problem before it happens. In a perfect world, all management would be proactive.

Reliability and Performance Monitor is a great tool for proactive network management. If you are creating baselines on a regular basis, you can identify system trends. For example, if you notice average CPU utilization increasing 5 percent every month, you can assume that within the next six months, you're going to have a problem. Before performance becomes so slow that your system is not responding, you can upgrade the hardware.

Testing Configuration Changes or Tuning Efforts

When you make configuration changes or tune your computer, you may want to measure the effects of those changes. When making configuration changes, the following recommendations apply:

- Make only one change at a time. If you are making configuration changes for tuning, and you make multiple changes at one time, it is difficult to quantify the effect of each individual change. In addition, some changes may have a negative impact that, if you have made multiple changes, may be difficult to identify.
- Repeat monitoring with each individual change you make. This will help you determine whether additional tuning is required.
- As you make changes, check the Event Viewer event log files. Some performance changes will generate events within Event Viewer that should be reviewed. Event Viewer is covered in more detail later in this chapter.
- If you suspect that network components are affecting performance, compare the performance of the network version with a version that runs locally.

Using Alerts for Problem Notification

The Reliability and Performance Monitor utility provides another tool for proactive management in the form of *alerts*. Through Data Collector Sets, you can specify alert thresholds (when a counter reaches a specified value) and have the utility notify you when these thresholds are reached.

For example, you could specify that if your logical disk has less than 10 percent of free space, you want to be notified. Once alerted, you can add more disk space or delete unneeded files before you run out of disk space. You will learn how to create alerts in the next section.

Using Reliability and Performance Monitor

The *Reliability and Performance Monitor* utility takes the place of Performance Logs and Alerts (PLA), Server Performance Advisor (SPA), and System Monitor. This utility is used to measure the performance of a local or remote computer on the network. Reliability and Performance Monitor enables you to do the following:

- Collect data from your local computer or remote computers on the network. You can collect data from a single computer or multiple computers concurrently.
- View data as it is being collected in real time, or historically from collected data.
- Have full control over the selection of what data will be collected, by selecting which specific objects and counters will be collected.
- Choose the sampling parameters that will be used, meaning the time interval that you want to use for collecting data points and the time period that will be used for data collection.
- Determine the format in which data will be viewed, in line, histogram bar, or report views.
- Create HTML pages for viewing data.
- Create specific configurations for monitoring data that can then be exported to other computers for performance monitoring.

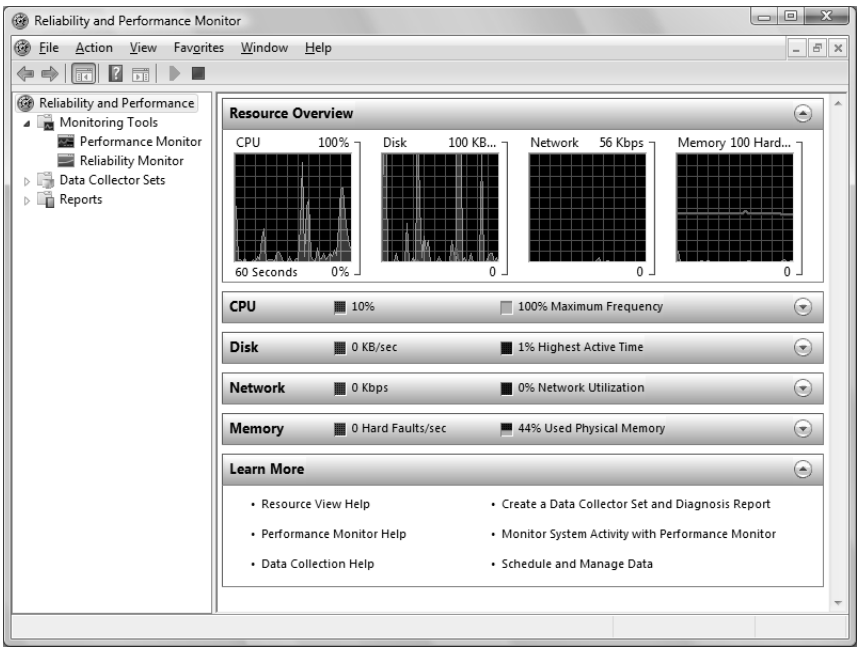
In order to view data on remote computers, you need to have administrative rights to the remote computer, and the Remote Registry Service must be enabled and running on the remote computer.

Through Reliability and Performance Monitor, you can view current data or data from a log file. When you view current data, you are monitoring real-time activity. When you view data from a log file, you are importing a log file from a previous session.

You can access Reliability and Performance Monitor through Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Reliability and Performance Monitor. Alternatively, you can simply run `perfmon.exe` from the command prompt. Figure 11.1 shows the main Reliability and Performance Monitor window when it is initially opened without configuration.

When you first start Reliability and Performance Monitor, the Resource Overview page is displayed. This page gives an excellent snapshot of what resources are being used in your computer. Notice that four resources are tracked: CPU, Disk, Network, and Memory. You can view detailed information about each resource by clicking the resource. For example, if you want to view how much of the CPU is being used by each process, click on the CPU resource. Detailed information will be displayed, as shown in Figure 11.2.

FIGURE 11.1 Reliability and Performance Monitor Resource Overview



Performance Monitor

For monitoring system activity other than what is provided by the Resource Overview, you must use Performance Monitor. Figure 11.3 shows the Performance Monitor window when it is initially opened without configuration.

Counters are listed at the bottom of the Performance Monitor window. By default, the % Processor Time counter is tracked for the local computer. The fields just above the counter list will contain data based on the counter that is highlighted in the list, as follows:

Last Displays the most current data.

Average Shows the average of the counter.

Minimum Shows the lowest value that has been recorded for the counter.

Maximum Shows the highest value that has been recorded for the counter.

Duration Shows how long the counter has been tracking data.

The following sections describe the three Performance Monitor views, how to add counters to track data, and how to configure Performance Monitor properties.

FIGURE 11.2 Reliability and Performance Monitor CPU Resource Overview

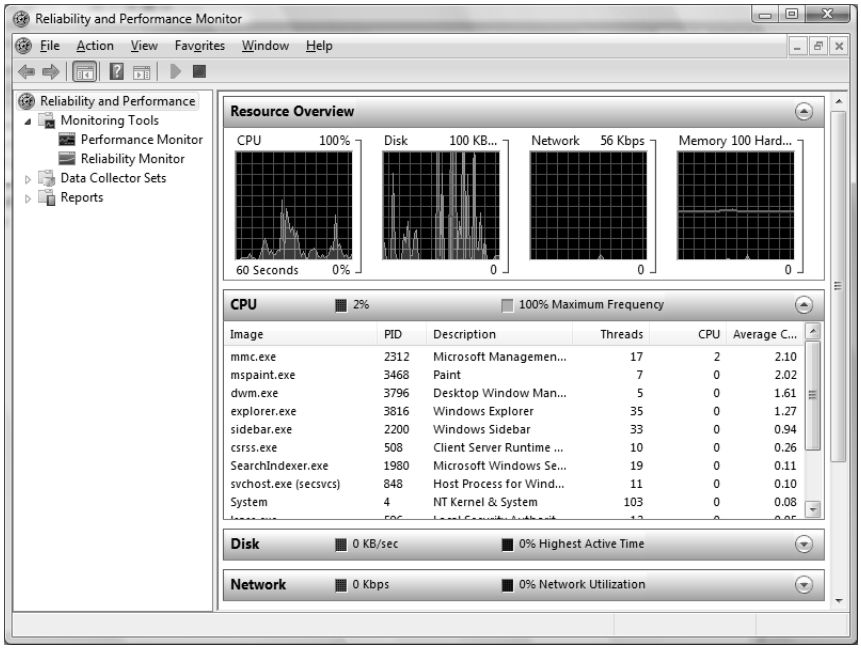
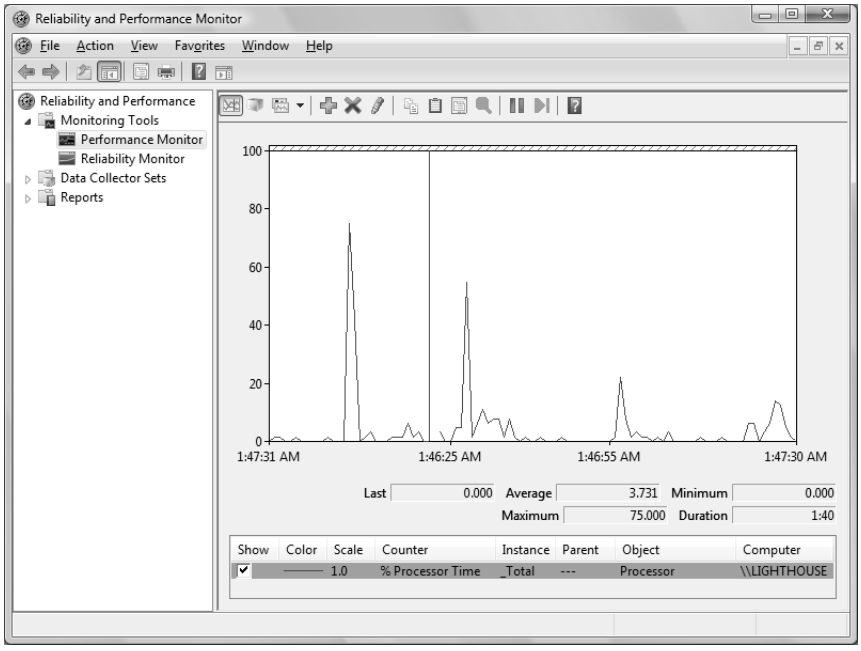


FIGURE 11.3 Performance Monitor



Selecting the Appropriate View

By clicking the Change Graph Type button on the Performance Monitor toolbar, you can see your data in one of three views:

Line view The line view, shown previously in Figure 11.3, is Performance Monitor's default view. It's useful for viewing a small number of counters in a graphical format. The main advantage of chart view is that you can see how the data has been tracked during the defined time period.

Histogram bar view The histogram view, shown in Figure 11.4, shows the Performance Monitor data in a bar graph. This view is useful for examining large amounts of data. However, it shows performance only for the current period. You do not see a record of performance over time, as you do with the line view.

Report view The report view, shown in Figure 11.5, offers a logical text-based report of all the counters that are being tracked through Performance Monitor. Only the current session's data is displayed. The advantage of report view is that it allows you to easily track large numbers of counters in real time.

FIGURE 11.4 The histogram bar view of Performance Monitor

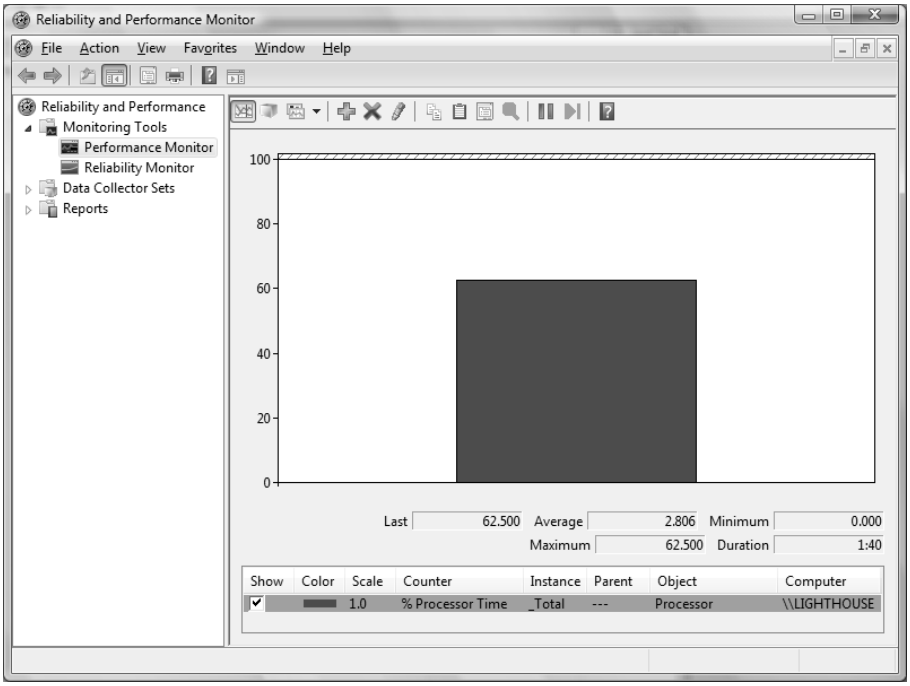
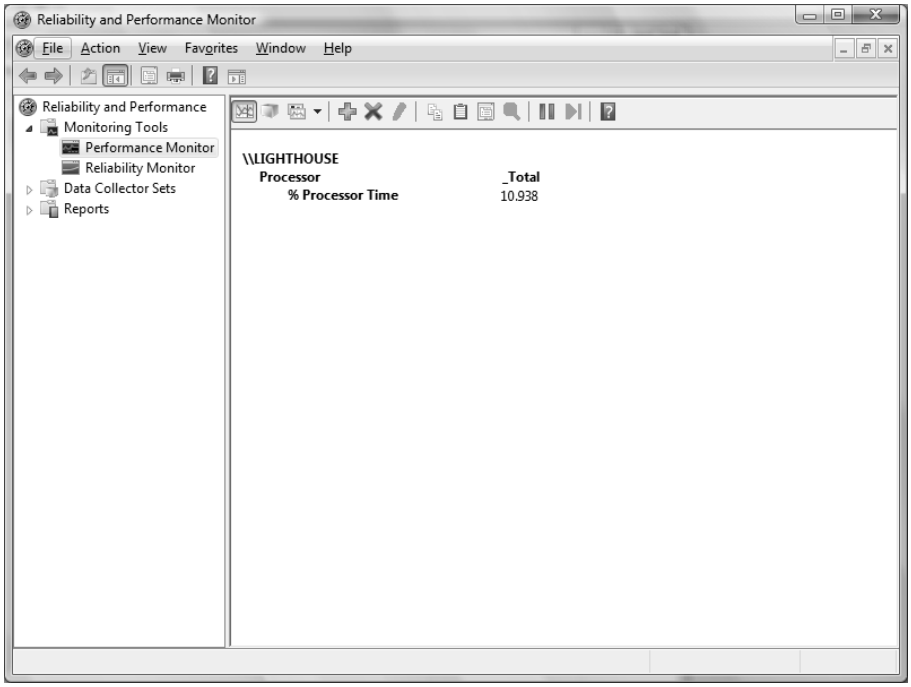


FIGURE 11.5 The report view of Performance Monitor



It is important to note that when you view data in real-time format, the data can appear skewed as applications and processes are started. It is typically more useful to view data as an average over a specified interval.

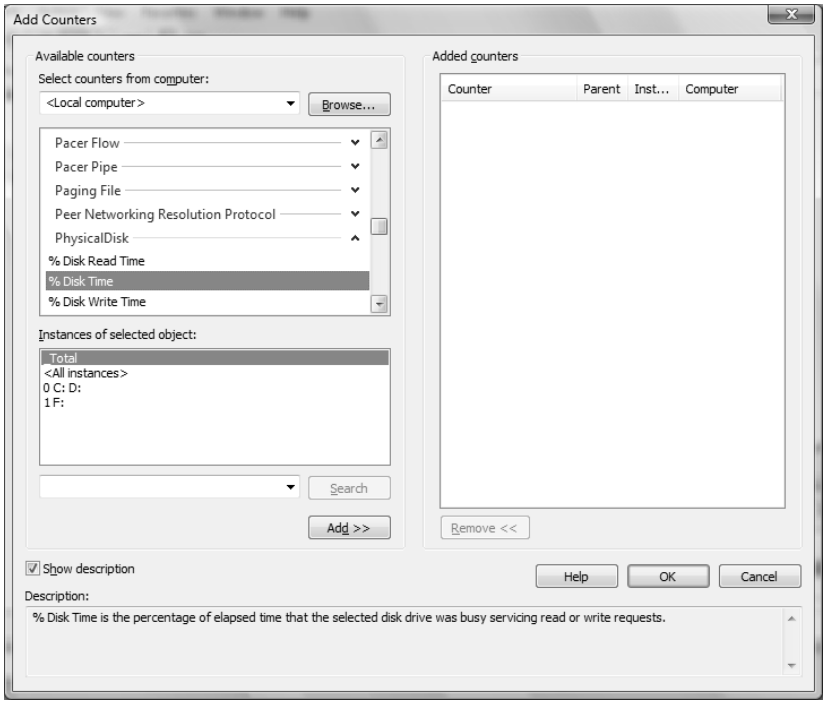
Adding Counters

As mentioned earlier, you must add *counters* to Performance Monitor to track data. To add counters, use the following steps:

1. In Performance Monitor, click the Add button on the toolbar, which looks like a green plus sign (+). This brings up the Add Counters dialog box (Figure 11.6).

To see information about a specific counter, in the Add Counters dialog box select the counter from the list and select the Show Description check box beneath the list. Performance Monitor will display text regarding the highlighted counter.

FIGURE 11.6 The Add Counters dialog box



2. In the Add Counters dialog box, ensure that the Select Counters from Computer drop-down list displays <Local Computer> so that you can monitor the local computer. Alternatively, to select counters from a specific computer, pick a computer from the drop-down list.

   You can monitor remote computers if you have administrative permissions. This option is useful when you do not want the overhead of Performance Monitor running on the computer you are trying to monitor.

3. Select a performance object from the drop-down list. All Windows Vista system resources are tracked as performance objects, such as Cache, Memory, Paging File, Process, and Processor.

   All the objects together represent your total system. Some performance objects exist on all Windows Vista computers; other objects appear only if specific processes or services are running. For example, if you want to track the physical disk's level of activity, choose the PhysicalDisk performance object.

4. Select the counter or counters within the performance object that you want to track. Each performance object has an associated set of counters. Counters are used to track specific information regarding a performance object. For example, the PhysicalDisk performance

object has a % Disk Time counter, which will tell you how busy a disk has been in servicing read and write requests. PhysicalDisk also has % Disk Read Time and % Disk Write Time counters, which show you what percentage of disk requests are read requests and what percentage are write requests, respectively.

You can select multiple counters of the same performance object by Shift-clicking contiguous counters or Ctrl-clicking noncontiguous counters.

5. Select <All Instances> to track all the associated instances, or pick specific instances from the list box.

   An instance is a mechanism that allows you to track the performance of a specific object when you have more than one item associated with a specific performance object. For example, suppose your computer has two physical drives. When you track the PhysicalDisk performance object, you can track one or both of your drives. If a counter has more than one instance, you can monitor the sum of all of the instances by selecting the _Total option.
6. Click the Add button to add the counters for the performance object.
7. Repeat steps 2 through 6 to specify any additional counters you want to track. When you have finished, click OK.

After you've added counters, you can select a specific counter by highlighting it in Performance Monitor. To highlight a counter, click it and then click the Highlight button (which looks like a highlighter) on the Performance Monitor toolbar, or select the counter and press Ctrl+H.

To stop showing data for a counter, deselect the check box under Show for that counter. To remove a counter, highlight it in Performance Monitor and click the Delete button on the toolbar. The Delete button looks like a red X.

Managing Performance Monitor Properties

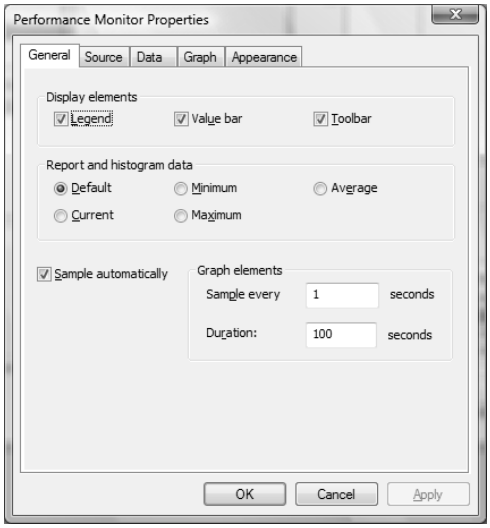
To configure the Performance Monitor properties, click the Properties button on the Performance Monitor toolbar. The Performance Monitor Properties dialog box has five tabs: General, Source, Data, Graph, and Appearance. The properties you can configure on each of these tabs are described in the following sections.

General Properties

The General tab of the Performance Monitor Properties dialog box (Figure 11.7) contains the following options:

- The display elements that will be used: legend, value bar, and/or toolbar
- The data that will be displayed: default (for reports or histograms, this is current data; for logs, this is average data), current, minimum, maximum, or average
- How often the data is updated, in seconds

FIGURE 11.7 Performance Monitor Properties, General tab



Source Properties

The Source tab, shown in Figure 11.8, allows you to specify the data source. This can be current activity, or it can be data that has been collected in a log file or database. If you import data, you can specify the time range that you wish to view.

Data Properties

The Data tab, shown in Figure 11.9, lets you specify the counters that you wish to track. You can add and remove counters by clicking the Add and Remove buttons. You can also select a specific counter and define the color, scale, width, and style that are used to represent the counter in the graph.

Graph Properties

The Graph tab, shown in Figure 11.10, contains the following options, which can be applied to the line or histogram bar view:

- Whether the data will scroll or wrap (line view only)
- A title
- A vertical axis label
- Whether you will show a vertical grid, a horizontal grid, vertical scale numbers, and/or time axis labels
- The minimum and maximum numbers for the vertical scale

FIGURE 11.8 Performance Monitor Properties, Source tab

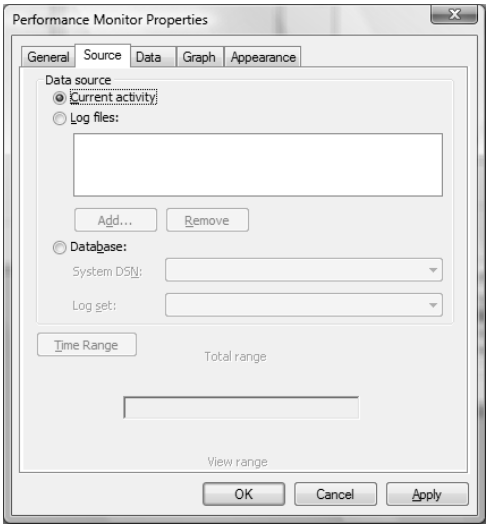
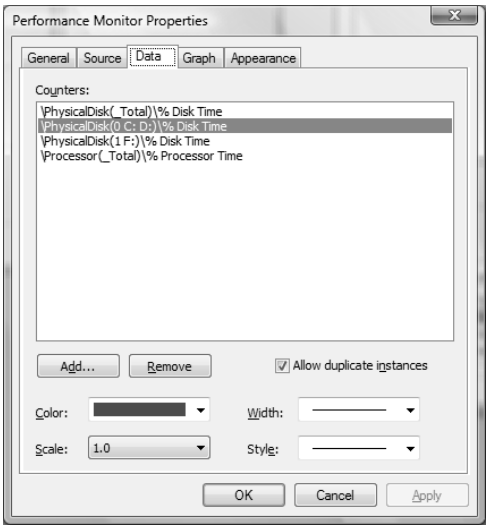


FIGURE 11.9 Performance Monitor Properties, Data tab



Appearance Properties

The Appearance tab of the Performance Monitor Properties dialog box, shown in Figure 11.11, has options for customizing the colors and fonts used in the Performance Monitor display.

FIGURE 11.10 Performance Monitor Properties, Graph tab

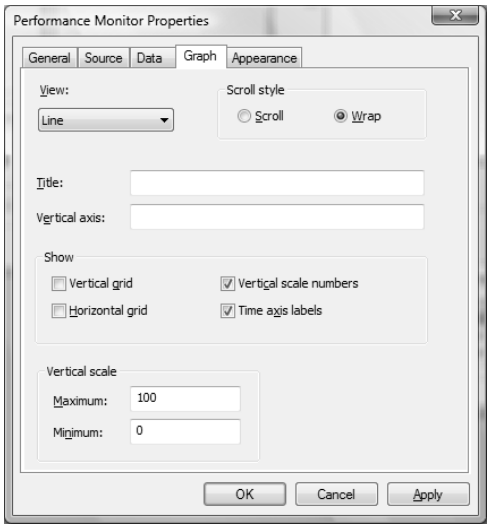
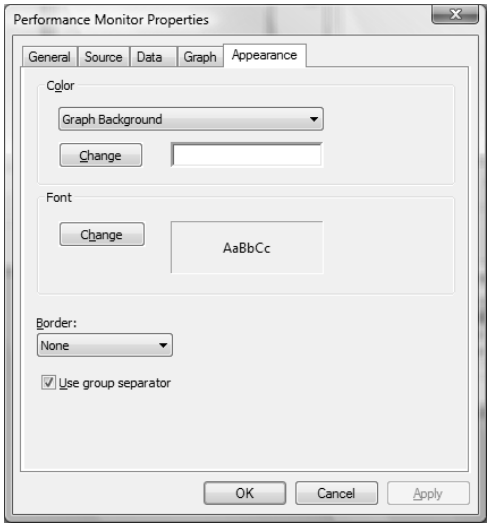


FIGURE 11.11 Performance Monitor Properties, Appearance tab



The following sections describe using Performance Logs and Alerts and how to manage system performance and optimize the system memory, processor, disk subsystem, and network subsystem.

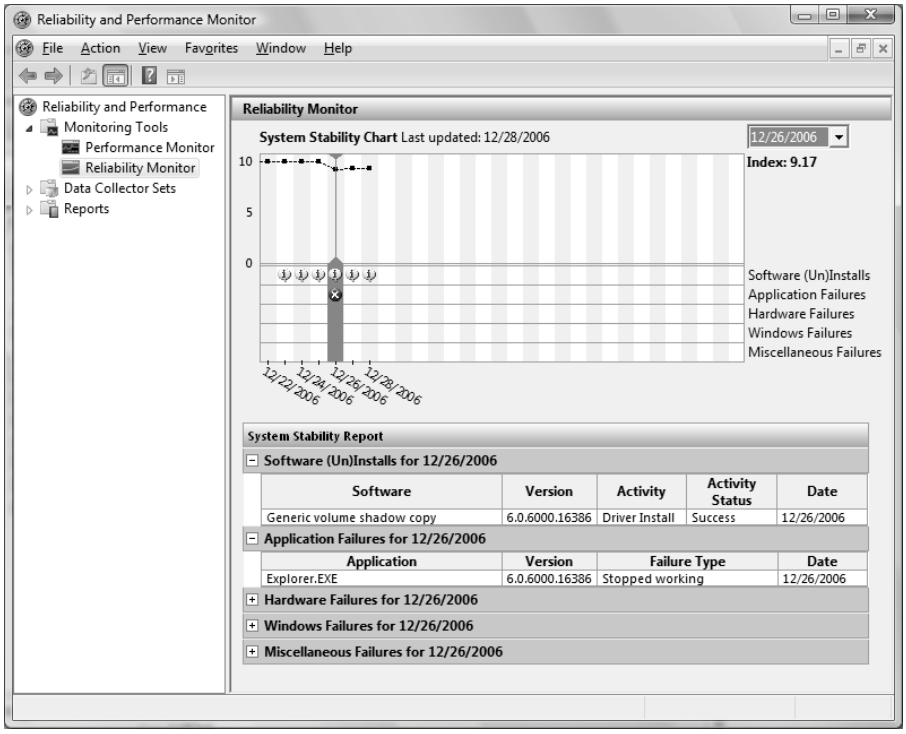
Using Reliability Monitor

Reliability Monitor is a new feature in Windows Vista that provides an overview of the stability of the computer. Figure 11.12 shows Reliability Monitor.

If something is causing system instability, Reliability Monitor can provide details about the problem. This data is collected and stored in the following five categories:

- Software (Un)Installs: Includes Windows updates and drivers
- Application Failures: Programs that hang or crash
- Hardware Failures: Includes disk and memory failures
- Windows Failures: Includes operating system and boot failures
- Miscellaneous Failures: Includes unexpected shutdowns

FIGURE 11.12 Reliability Monitor



Details about failures during the specified time period can be viewed by clicking the plus sign (+) next to each category. The time period can be changed by clicking the drop-down list box in the upper-right corner and selecting a date. Information for all dates can be viewed by selecting Select All.

Reliability Monitor measures the amount of system stability and calculates the Stability Index, which is a rating from 0 to 10. A score of 10.00 indicates that your computer system has experienced no stability problems.

If you notice a recurring problem, you might want to run Problem Reports and Solutions and check Event Viewer. If a driver is bad, check Device Manager and run Windows Update. If you are having disk failures, check your volume for errors, and you should back up your data using Backup and Restore Center as soon as possible. For memory failures, you can run the Memory Diagnostics Tool.

We cover Windows Update in Chapter 1, "Getting Started with Windows Vista." We examine Device Manager in Chapter 3, "Configuring the Windows Vista Environment." We discuss disk management tools, such as Disk Defragmenter and Disk Cleanup, in Chapter 7, "Configuring Disks." We cover Problem Reports and Solutions, Event Viewer, Backup and Restore Center and the Memory Diagnostic Tool later in this chapter.

Using Data Collector Sets

The Data Collector Set portion of Reliability and Performance Monitor is displayed in Figure 11.13. Data collector sets are used to collect data into a log so that the data can be reviewed. You can view the log files with Performance Monitor, as described in the previous section.

Data collector sets can collect the following data:

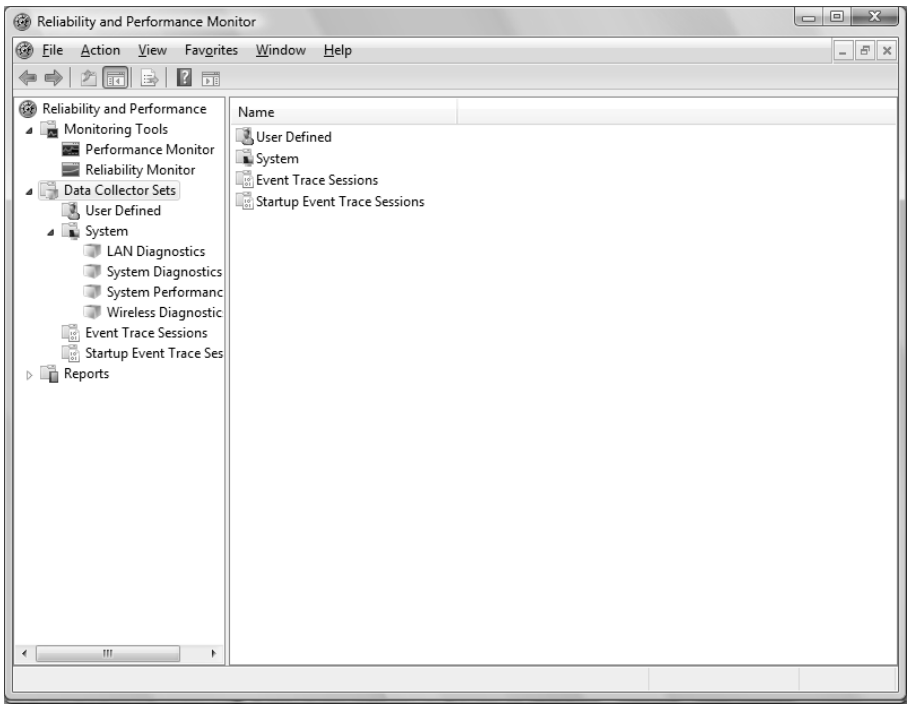
- Performance counters
- Event trace data
- System configuration information

Windows Vista includes the following four data collector sets that are stored within the System subfolder:

- LAN Diagnostics
- System Diagnostics
- System Performance
- Wireless Diagnostics

These data collector sets track multiple counters. You can also create your own user-defined data collector sets. You can view the reports from these data collector sets within the Reports folder in Reliability and Performance Monitor. The following sections describe how to use data collector sets.

FIGURE 11.13 Data Collector Sets



Creating a User-Defined Data Collector Set

Performance counter logs record data about hardware usage and the activity of system services. You can configure logging to occur manually or on a predefined schedule.

To create a data log, take the following steps:

1. Expand Data Collector Sets, right-click User Defined, select New, then select Data Collector Set from the pop-up menu.
2. In the Create New Data Collector Set dialog box that appears, type a name for the collector set. For example, you might give the log a name that indicates its type and the date, such as **Counter*mmddyy***. You can also select whether to create the set from a template or to create it manually. Then click the Next button.
3. If you chose to create the set from a template, follow the prompts to create the set. After the set is created, you can modify it. If you chose to create the set manually, you will be asked whether you want to create data logs or a Performance Counter Alert. Data logs can consist of the following types of data:
   - Performance counters

- Event trace data
- System configuration information (Registry keys)

After you have selected which data you want to collect, click Next.

4. Configure the performance counters, trace data, and Registry keys that you want to collect, clicking Next after each data type.
5. You will be asked where to save the data. Browse to the location, click OK, then click Next.
6. You will be asked under which user account the data collector set should run, and whether the data collector set should be edited, started, or saved. After you make your selections, click Finish.

Creating an Alert

Alerts can be generated when a specific counter rises above or falls below a specified value. You can configure alerts to log an entry in the application event log and/or start a data collector set. Creating an alert is similar to creating a performance counter data log except you are required to specify the alert conditions. For example, you might configure a performance counter alert that will log an entry whenever the % Free Space counter for C: falls below 5%. After you create the alert, you can modify the alert parameters by right-clicking the data collector and selecting Properties.

Managing System Performance

By analyzing data, you can determine whether any resources are placing an excessive load on your computer that is resulting in a system slowdown. Here are some of the causes of poor system performance:

- A resource is insufficient to handle the load that is being placed upon it, and the component may need to be upgraded, or additional components may be required.
- If a resource has multiple instances, the resources may not be evenly balancing the workload, and the workload may need to be balanced over the multiple instances more effectively.
- A resource might be malfunctioning. In this case, the resource should be repaired or replaced.
- A specific program might be allocated resources improperly or inefficiently, in which case the program needs to be rewritten or another application should be used.
- A resource might be configured improperly and causing excessive resource usage, and needs to be reconfigured.

The four main subsystems that should be monitored are

- The memory subsystem
- The processor subsystem

- The disk subsystem
- The network subsystem

Each of these subsystems is examined in greater detail in the following sections.

Monitoring and Optimizing Memory

When the operating system needs a program or process, the first place it looks is in physical memory. If the required program or process is not in physical memory, the system looks in logical memory (the *page file*). If the program or process is not in logical memory, the system then must retrieve the program or process from the hard disk. It can take thousands of times longer to access information from the hard disk than to get it from physical RAM. If your computer is using excessive paging, that is an indication that your computer does not have enough physical memory.

Insufficient memory is the most likely cause of system bottlenecks. If you have no idea what is causing a system bottleneck, memory is usually a good place to start checking. To determine how memory is being used, you need to examine two areas:

Physical memory The physical RAM you have installed on your computer. You can't have too much memory. It's actually a good idea to have more memory than you think you will need just to be on the safe side. As you've probably noticed, each time you add or upgrade applications, you require more system memory.

Page file Logical memory that exists on the hard drive. If you are using excessive paging (swapping between the page file and physical RAM) or hard page faults, it's a clear sign that you need to add more memory.

The first step in memory management is determining how much memory your computer has installed and what the appropriate memory requirements are based on the operating system requirements and the applications and services you are running on your computer.

In this book, we use the following format for describing performance object counters: *performance object* > *counter*. For example, Memory > Available MBytes denotes the Memory performance object and the Available MBytes counter.

Key Counters to Track for Memory Management

Following are the three most important counters for monitoring memory:

Memory > Available MBytes Measures the amount of physical memory that is available to run processes on the computer. If this number is less than 20% of your installed memory, it indicates that you might have an overall shortage of physical memory for your computer, or you possibly have an application that is not releasing memory properly. You should consider adding more memory or evaluating application memory usage.

Memory > Pages/Sec Shows the number of times the requested information was not in memory and had to be retrieved from disk. This counter's value should be below 20; for optimal performance, it should be 4 or 5. If the number is above 20, you should add memory or research paging file use more thoroughly. Sometimes a high Pages/Sec counter is indicative of a program that is using a memory-mapped file.

Paging File > % Usage Indicates the percentage of the allocated page file that is currently in use. If this number is consistently over 70%, you may need to add more memory or increase the size of the page file. You should track this counter in conjunction with Available MBytes and Pages/Sec.

These counters work together to show what is happening on your system. Use the Paging File > % Usage counter value in conjunction with the Memory > Available MBytes and Memory > Pages/Sec counters to determine how much paging is occurring on your computer.

If you suspect that one of your applications has a memory leak, you should monitor the following counters:

- Memory > Available Bytes
- Memory > Committed Bytes
- Process > Private Bytes (for the application you suspect is leaking memory)
- Process > Working Set (for the application you suspect is leaking memory)
- Process > Handle Count (for the application you suspect is leaking memory)
- Memory > Pool Nonpaged Bytes

Managing the Windows Vista Page File

Typically, if your computer is experiencing excessive paging, the best way to optimize memory is to add more physical memory. However, there are some other options for managing the paging file for better performance. They include

- Spreading the page file across multiple hard disks, which allows the disk I/O associated with paging to be spread over multiple disk I/O channels, for faster access.
- If you have sufficient disk space, increasing the size of the page file. By default, Windows Vista creates a page file (`pagefile.sys`) and manages the size automatically. You would want to consider increasing the page file size if the Paging File > % Usage counter is near 100%.

The main counters for tracking page file usage are

- Paging File > % Usage
- Paging File > % Usage Peak

If a manually configured page file reaches the maximum size, the user will see a warning displayed, and the system might halt. This is another reason to monitor the page file and increase the size if the paging file is not managed automatically by Windows Vista.

You will learn how to view and manage the page file later in this chapter in the "Using the System Tool in Control Panel" section. Only administrators can manage this option.

Tuning and Upgrading Memory

If you suspect that you have a memory bottleneck, the following options can be used to tune or upgrade memory:

- Increase the amount of physical memory that is installed on the computer.
- If your computer has multiple disk channels, create multiple page files across the disk channels.
- Verify that your page file is sized correctly.
- Try to run less memory-intensive applications.
- Try to avoid having your page file on the same partition as the system files.

In Exercise 11.1, you will monitor your computer's memory subsystem.

EXERCISE 11.1

Monitoring System Memory

1. Select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Reliability and Performance Monitor.
2. In the Performance Monitor window, click the Add button on the toolbar.
3. In the Add Counters dialog box, specify the following performance objects and counters:

   Select Memory from the Performance Object drop-down list, choose Available MBytes in the counter list box, and click the Add button.

   Select Memory from the Performance Object drop-down list, choose Pages/Sec in the counter list box, and click Add.

   Select Paging File from the Performance Object drop-down list, choose % Usage in the counter list box, click _Total in the Instances list box, and click Add.
4. Click OK. You should see a chart showing how your computer's memory is being used.
5. To generate some activity, select Start ➢ Windows Meeting Space. Close Windows Meeting Space. Open Windows Meeting Space again and then close it. The first time you opened Windows Meeting Space, you should have seen a spike in the Memory > Pages/Sec counter and a much lower spike (if any) the second time you accessed Windows Meeting Space. This occurred because the application had to be retrieved from disk the first time you accessed it; the second time you accessed it, it was already in memory.

EXERCISE 11.1 *(continued)*

6. Note the Paging > % Usage counter. If this counter is below 70%, your system is not using excessive paging.
7. Note the Memory > Available MBytes counter. If this counter is above 20% of your installed memory, you should have sufficient RAM.

Leave Reliability and Performance Monitor open, for use again in Exercise 11.2.

Real World Scenario

Using Performance Monitor to Identify Bottlenecks

You are the system administrator of a large network. The accounting department has just started using a new accounting application that runs on the department manager's local computer. The manager is complaining about the slowness of this application and says she needs a new computer.

You decide to use Performance Monitor to find out why her computer is responding so slowly. You see that the processor utilization is at 10% (low). You also can tell that the system is using excessive paging based on the Memory > Pages/Sec counter, currently showing at 25. Considering this information, you determine that for the accounting manager's computer to work efficiently with the application, the computer needs a memory upgrade.

Performance Monitor helps you measure the performance of various parts of your system, allowing you to identify system bottlenecks scientifically.

Monitoring and Optimizing the Processor

Processor bottlenecks can develop when the threads of a process require more processing cycles than are currently available. In this case, the process will wait in a processor queue and system responsiveness will be slower than if process requests could be immediately served. The most common causes of processor bottlenecks are processor-intensive applications and other subsystem components that generate excessive processor interrupts (for example, disk or network subsystems).

In a workstation environment, processors are usually not the source of bottlenecks. You should still monitor this subsystem to make sure that processor utilization is at an efficient level.

Key Counters to Track for Processor

You can track processor utilization through the Processor and System objects to determine whether a processor bottleneck exists. The following are the three most important counters for monitoring the system processor:

Processor > % Processor Time Measures the time that the processor spends responding to system requests. If this value is consistently above an average of 85%, you may have a processor bottleneck. The Processor > % User Time and Processor > % Privileged Time counters combine to show the total % Processor Time counter. You can monitor these counters individually for more detail.

Processor > Interrupts/Sec Shows the average number of hardware interrupts received by the processor each second. If this value is more than 3,000 on a Pentium 4 computer, you might have a problem with a program or hardware that is generating spurious interrupts.

System > Processor Queue Length Used to determine whether a processor bottleneck is due to high levels of demand for processor time. If a queue of two or more items exists for an extended period of time, a processor bottleneck may be indicated.

If you suspect that a processor bottleneck is due to excessive hardware I/O requests, then you should also monitor the System > File Control Bytes/Sec counter.

Tuning and Upgrading the Processor

If you suspect that you have a processor bottleneck, you can try the following solutions:

- Use applications that are less processor-intensive.
- Upgrade your processor.
- If your computer supports multiple processors, add one. Windows Vista Business, Windows Vista Enterprise, and Windows Vista Ultimate support two physical processors (regardless of the number of cores per processor), which will help if you use multithreaded applications. You can also use processor affinity to help manage processor-intensive applications.

In Exercise 11.2, you will monitor your computer's processor. This exercise assumes that you have completed the previous exercise in this chapter.

EXERCISE 11.2

Monitoring the System Processor

1. If Reliability and Performance Monitor is not already open, select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Reliability and Performance Monitor.
2. In the Performance Monitor window, click the Add button on the toolbar.

EXERCISE 11.2 *(continued)*

3. In the Add Counters dialog box, specify the following performance objects and counters:

   Select Processor from the Performance Object drop-down list, select % Processor Time in the counter list box, select _Total in the Instances list box, and click Add.

   Select Processor from the Performance Object drop-down list, select Interrupts/Sec in the counter list box, select _Total in the Instances list box, and click Add.

4. Click OK. You should see these counters added to your chart.

5. To generate some activity, open Internet Explorer, pull up a website, and close Internet Explorer. You should see that the % Processor Time counter spiked during this process.

6. Note the Processor > % Processor Time counter. If this counter's average is below 85%, you do not have a processor bottleneck.

7. Note the Processor > Interrupts/Sec counter. If this counter is below 3,000 on a Pentium 4 computer, you probably do not have any processes or hardware devices that are generating excessive interrupts.

Leave Reliability and Performance Monitor open, for use again in Exercise 11.3.

Monitoring and Optimizing the Disk Subsystem

Disk access is the amount of time your disk subsystem takes to retrieve data that is requested by the operating system. The two factors that determine how quickly your disk subsystem will respond to system requests are the average disk access time on your hard drive and the speed of your disk controller.

Key Counters to Track for the Disk Subsystem

You can monitor the PhysicalDisk object, which is the sum of all logical drives on a single physical drive, or you can monitor the LogicalDisk object, which represents a specific logical disk. Here are the most important counters for monitoring the disk subsystem:

PhysicalDisk > % Disk Time and LogicalDisk > % Disk Time Shows the amount of time the disk is busy because it is servicing read or write requests. If the disk is busy more than 90% of the time, you will improve performance by adding another disk channel and splitting the disk I/O requests between the channels.

PhysicalDisk > Current Disk Queue Length and LogicalDisk > Current Disk Queue Length Indicates the number of outstanding disk requests that are waiting to be processed. On average, this value should be less than 2.

LogicalDisk > % Free Space Specifies how much free disk space is available. This counter should be at least 15%.

Tuning and Upgrading the Disk Subsystem

When you suspect that you have a disk subsystem bottleneck, the first thing you should check is your memory subsystem. Insufficient physical memory can cause excessive paging, which in turn affects the disk subsystem. If you do not have a memory problem, you can try the following solutions to improve disk performance:

- Use faster disks and controllers.
- Confirm that you have the latest drivers for your disk host adapters.
- Use disk striping to take advantage of multiple I/O channels.
- Balance heavily used files on multiple I/O channels.
- Add another disk controller for load balancing.
- Use Disk Defragmenter to consolidate files so that disk space and data access are optimized.
- If you are on a network, distribute applications that have high disk I/O through the Distributed File System (DFS) to balance workload.

In Windows NT 4, you enabled all disk counters through the `Diskperf -y` command. Physical and logical disk counters are automatically enabled in Windows Vista.

In Exercise 11.3, you will monitor your disk subsystem. This exercise assumes that you have completed the previous exercises in this chapter.

EXERCISE 11.3

Monitoring the Disk Subsystem

1. If Reliability and Performance Monitor is not already open, select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Reliability and Performance Monitor.
2. In the Performance Monitor window, click the Add button on the toolbar.
3. In the Add Counters dialog box, specify the following performance objects and counters:

   Select PhysicalDisk from the Performance Object drop-down list, select % Disk Time from the counter list box, select _Total in the Instances list box, and click Add.

   Select PhysicalDisk from the Performance Object drop-down list, select Current Disk Queue Length from the counter list box, select _Total in the Instances list box, and click Add.

   Select LogicalDisk from the Performance Object drop-down list, select % Idle Time from the counter list box, select _Total in the Instances list box, and click Add.

EXERCISE 11.3 *(continued)*

4. Click OK. You should see these counters added to your chart.
5. To generate some activity, open and close some applications and copy some files between the C: drive and D: drive.
6. Note the PhysicalDisk > % Disk Time counter. If this counter's average is below 90%, you are not generating excessive requests to this disk.
7. Note the PhysicalDisk > Current Disk Queue Length counter. If this counter's average is below 2, you are not generating excessive requests to this disk.

Leave Reliability and Performance Monitor open; you will use this utility again in Exercise 11.4.

You can monitor the amount of free disk space on your logical disk through the LogicalDisk > % Free Space counter. This counter can also be used as an alert. For example, you might set an alert to notify you when LogicalDisk > % Free Space on drive C: is under 10%.

Monitoring and Optimizing the Network Subsystem

Windows Vista does not have a built-in mechanism for monitoring the entire network. However, you can monitor and optimize the traffic that is generated on the specific Windows Vista computer. You can monitor the network interface (your network card), and you can monitor the network protocols that have been installed on your computer.

Network bottlenecks are indicated when network traffic exceeds the capacity that can be supported by the local area network (LAN). Typically, you would monitor this activity on a network-wide basis—for example, with the Network Monitor utility that ships with Windows Server 2003.

Key Counters to Track for the Network Subsystem

If you are using the Performance Monitor utility to monitor local network traffic, the following two counters are useful for monitoring the network subsystem:

Network Interface > Bytes Total/Sec Measures the total number of bytes sent or received from the network interface and includes all network protocols.

TCPv4 > Segments/Sec Measures the number of bytes sent or received from the network interface and includes only the TCPv4 protocol.

Normally, you monitor and optimize the network subsystem from a network perspective rather than from a single computer. For example, you can use a network protocol analyzer to monitor all traffic on the network to determine whether the network bandwidth is acceptable for your requirements and that network bandwidth is saturated.

Tuning and Upgrading the Network Subsystem

The following suggestions can help to optimize and minimize network traffic:

- Use only the network protocols you need.
- Use network cards that take full advantage of your bus width.
- Use faster network cards—for example, 100Mbps Ethernet or 1Gbps Ethernet instead of 10Mbps Ethernet.

In Exercise 11.4, you will monitor your network subsystem. This exercise assumes that you have completed the previous exercises in this chapter.

EXERCISE 11.4

Monitoring the Network Subsystem

1. If Reliability and Performance Monitor is not already open, select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Reliability and Performance Monitor.
2. In the Performance Monitor window, click the Add button on the toolbar.
3. In the Add Counters dialog box, specify the following performance objects and counters:

   Select Network Interface from the Performance Object drop-down list, select Bytes Total/Sec in the counter list box, select <All Instances>, and click Add.

   Select TCPv4 from the Performance Object drop-down list, select Segments/Sec from the counter list box, and click Add.
4. Click OK. You should see these counters added to your chart.
5. To generate some activity, open Internet Explorer and visit a few websites.
6. Note the data collected by your counters.

Leave Reliability and Performance Monitor open; you will use this utility again in Exercise 11.5.

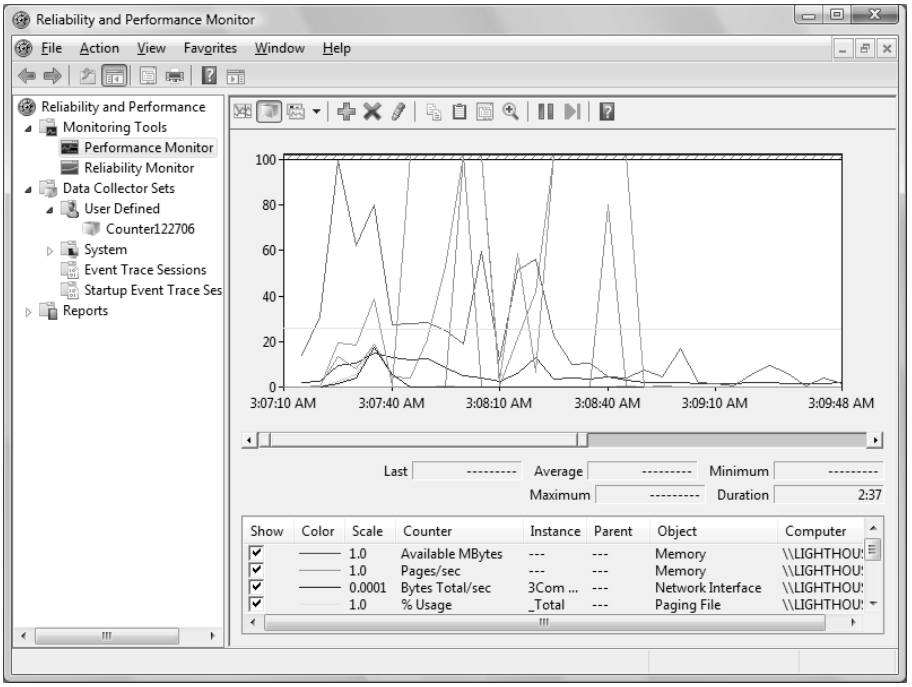
Creating Baseline Reports

As explained earlier in this chapter, baselines show how your server is performing at a certain time. By taking baselines at regular intervals and also whenever you make changes to the system's configuration, you can monitor your workstation's performance over time.

You can create baselines by setting up a counter log file in the Reliability and Performance Monitor utility. After you've created the baseline log file, you can view it in Performance Monitor, as shown in Figure 11.14.

In Exercise 11.5, you will create a baseline report for your computer.

FIGURE 11.14 Viewing a performance baseline in Performance Monitor



EXERCISE 11.5

Creating a Baseline Report

1. If Reliability and Performance Monitor is not already open, select Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Reliability and Performance Monitor.

EXERCISE 11.5 *(continued)*

2. In the Performance Monitor window, expand Data Collector Sets, right-click User Defined, select New, and click Data Collector Set.
3. In the Create New Data Collector Set dialog box, type **Counter*mmddyy*** (replace *mmddyy* with the current month, date, and year) as the log name. Select Create Manually (Advanced), and click the Next button.
4. Select Create Data Logs, and select the check box next to Performance Counter. Click Next to continue.
5. Click the Add button. Add the following counters:

   Memory > Available MBytes

   Memory > Pages/Sec

   Paging File > % Usage (_Total)

   Processor > % Processor Time (_Total)

   Processor > Interrupts/Sec (_Total)

   PhysicalDisk > % Disk Time (_Total)

   PhysicalDisk > Current Disk Queue Length (_Total)

   Network Interface > Bytes Total/Sec (<All Instances>)

   TCPv4 > Segments/Sec
6. Click OK, and set the interval for sampling data to 5 seconds. Click Next to continue.
7. Specify the location where you want to save your log file. By default, the file will be stored in `C:\PerfLogs` if Windows Vista is installed on C:. Click Next to continue.
8. Click Start This Data Collector Set Now, then click Finish.
9. Generate some system activity: start and stop some applications, copy a few files, and browse websites using Internet Explorer for 1 or 2 minutes.
10. Stop the data collection by right-clicking Counter *mmddyy* and clicking Stop.
11. To view your log file, click Performance Monitor, then click the View Log Data icon in the Performance Monitor toolbar. Select Log Files, click Add, then double-click on the **Counter*mmddyy*** folder and subfolder until you see your log file. Select the log file and click Open. Click OK to continue.
12. Add the counters from the log file you created to see the data that was collected in your log.

Minimizing the Performance Effects of System Monitoring

The goal of monitoring system performance is to manage system performance. The system monitoring tools are designed to use minimal system resources; however, the following configurations can increase system overhead when you are using system monitoring tools:

- You run Reliability and Performance Monitor in graph mode, which uses more resources.
- You configure sampling to run at very frequent intervals (more than once every three seconds).
- You select a very large number of counters to track (you should track only key counters, not everything).
- By selecting a large number of counters and a frequent interval sample, you create very large log files, which will impact disk space and disk input/output usage. If you are monitoring disk usage, you should place the log files on a disk other than the one you are monitoring.

If you are creating a log file to be tracked over the following intervals, it is recommended that you set update intervals to the following values:

- Daily, every 3–5 minutes
- Weekly, every 15 minutes
- Monthly, every 2–3 hours

Memory Diagnostics Tool

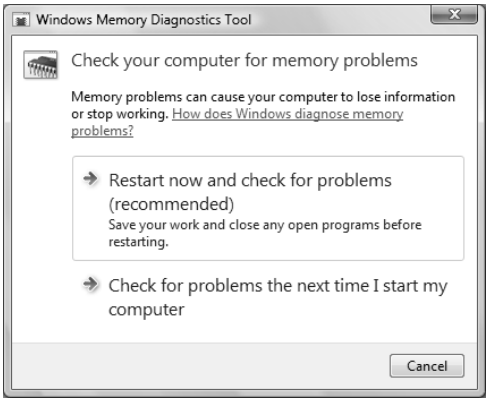
If you are having problems with your computer's memory, the *Memory Diagnostics Tool* will automatically launch. Alternatively, you can run the Memory Diagnostics Tool manually by clicking Start ➢ Control Panel ➢ Classic View ➢ Administrative Tools ➢ Memory Diagnostics Tool.

When you launch the Memory Diagnostics Tool, the dialog box in Figure 11.15 will be displayed. If you decide to check your memory now, your computer will restart and begin testing your memory. Otherwise, it will test the memory the next time you restart the computer. After the test is finished, Windows will start and the test results will be displayed after you log on.

If you are unable to boot your computer, you can launch the Memory Diagnostics Tool by following these steps:

1. Boot your computer using the Windows Vista media, or use the recovery partition instructions provided by your computer manufacturer.
2. When the Install Windows dialog box appears, select the language, time and currency format, and the keyboard or input method. Click Next to continue.

FIGURE 11.15 Memory Diagnostics Tool



3. The Install Now button will appear in the center of the screen. Click Repair Your Computer in the lower-left corner.
4. Select the operating system to recover and click Next. If you do not see your operating system, you might need to load your hard disk drivers by clicking the Load Drivers button.
5. The System Recovery Options dialog box will appear. You can choose one of the following options:
   - Startup Repair
   - System Restore
   - Windows Complete PC Restore
   - Windows Memory Diagnostic Tool
   - Command Prompt
6. Choose Windows Memory Diagnostic Tool to continue.
7. You will see a dialog box similar to Figure 11.15. Allow the Memory Diagnostics Tool to check your memory. Afterward, the computer will restart.

If you were not provided the Windows Vista media when you purchased your computer, the computer manufacturer might have placed the files on a recovery partition. Check with the manufacturer for more information.

Problem Reports and Solutions

Before Windows Vista, when an application error occurred, Dr. Watson would launch and would attempt to debug the error. Windows Vista has retired the good doctor and has replaced

him with *Problem Reports and Solutions*. If a problem occurs on your computer, such as an application hanging or a driver failing to load, Problem Reports and Solutions will record the error and allow you to check for potential solutions to your problem by sending the error to Microsoft, as shown in Figure 11.16. Any available solutions to your problem will then appear. If your problem is unique, sending information to Microsoft will allow them to know that the problem exists.

To open Problem Reports and Solutions, click Start ➢ Control Panel ➢ System and Maintenance ➢ Problem Reports and Solutions. The Problem Reports and Solutions dialog box will appear, as shown in Figure 11.17.

FIGURE 11.16 Sending error information to Microsoft

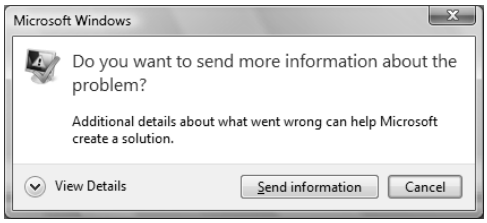
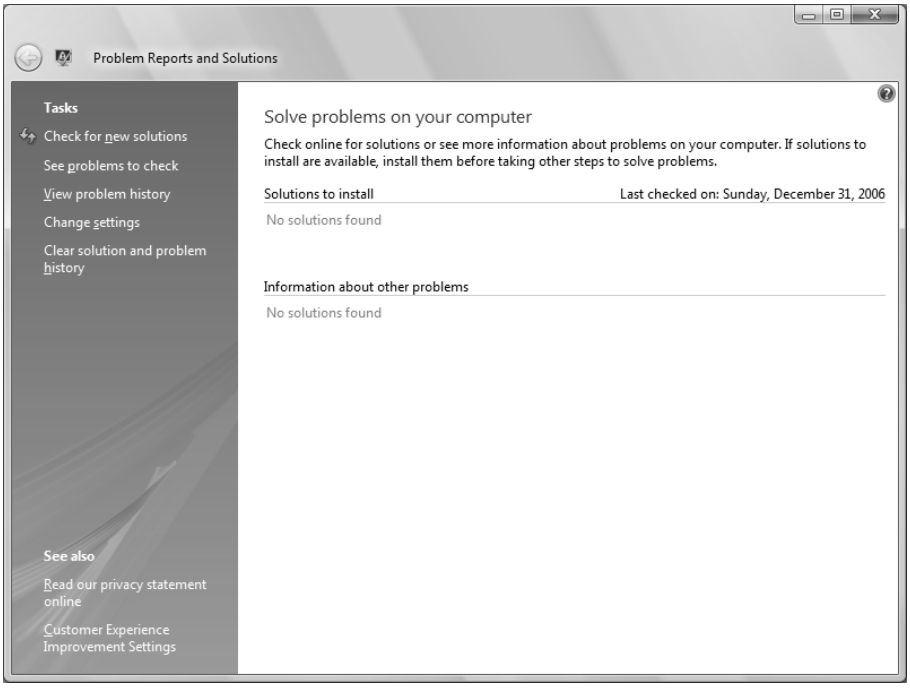


FIGURE 11.17 Problem Reports and Solutions



You can check for new solutions to existing problems, review new product reports, view your problem history, change whether to check for solutions automatically, and clear your solution and problem history. Checking for solutions to previous problems can be helpful because new solutions might have become available since the last time you checked.

Using Tools to Discover System Information

Windows Vista contains many other tools to discover system information about your computer. We will discuss the following tools in this section:

- System Information
- Task Manager
- Performance Information and Tools

System Information

The *System Information* utility, shown in Figure 11.18, is used to show details about your hardware, software, and resources. To launch this utility, run `msinfo32.exe` from the command prompt. As you can see, a great deal of information can be found using this application. Click the fields in the left pane, and details will be displayed in the right pane. You can also search for a term by typing it in the Find What field at the bottom of the page.

Task Manager

The *Task Manager* utility shows the applications and processes that are currently running on your computer, as well as CPU and memory usage information. To access Task Manager, press Ctrl+Alt+Delete and click Start Task Manager. Alternatively, right-click an empty area in the taskbar and select Task Manager from the context menu.

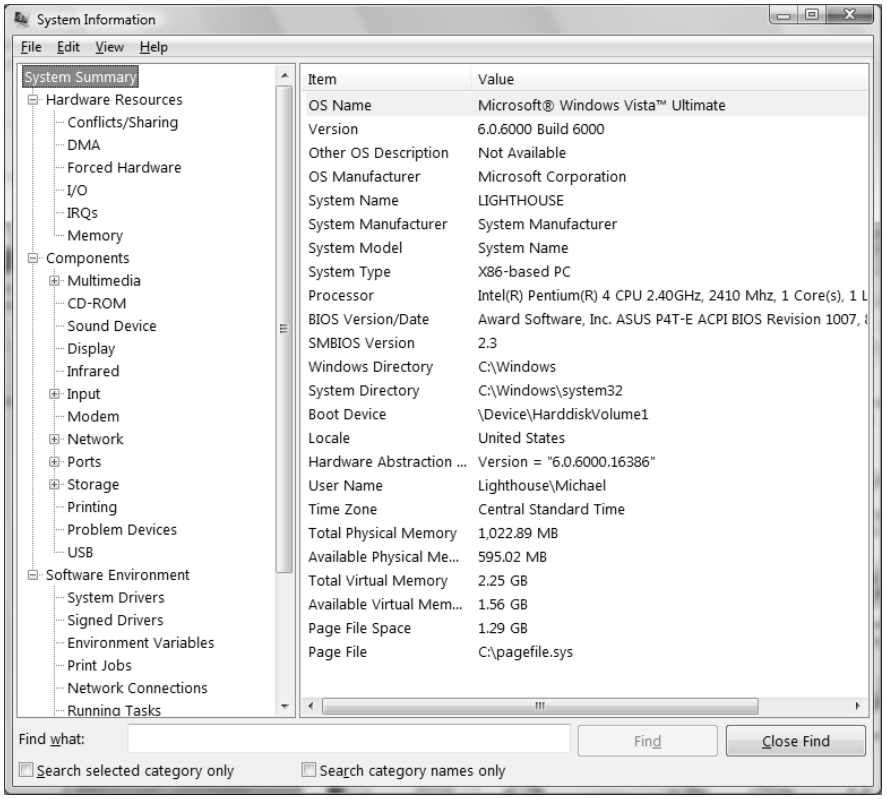
The Task Manager dialog box has six main tabs: Applications, Processes, Services, Performance, Networking, and Users. These options are covered in the following subsections.

By default, Task Manager stays on top of other windows.

Managing Application Tasks

The Applications tab of the Task Manager dialog box, shown in Figure 11.19, lists all of the applications that are currently running on the computer. For each task, you will see the name of the task and the current status (running, not responding, or stopped).

FIGURE 11.18 System Information



To close an application, select it and click the End Task button at the bottom of the dialog box. To make the application window active, select it and click the Switch To button. If you want to start an application that isn't running, click the New Task button and specify the location and name of the program you wish to start.

Managing Process Tasks

The Processes tab of the Task Manager dialog box, shown in Figure 11.20, lists all the processes that are currently running on the computer. This is a convenient way to get a quick look at how your system is performing.

For each process, you will see the Image Name (the name of the process), the User Name (the user account that is running the process), CPU (the amount of CPU utilization for the process), Memory (Private Working Set) (the amount of memory that is being used by the process), and Description (a description of the process).

FIGURE 11.19 Task Manager, Applications tab

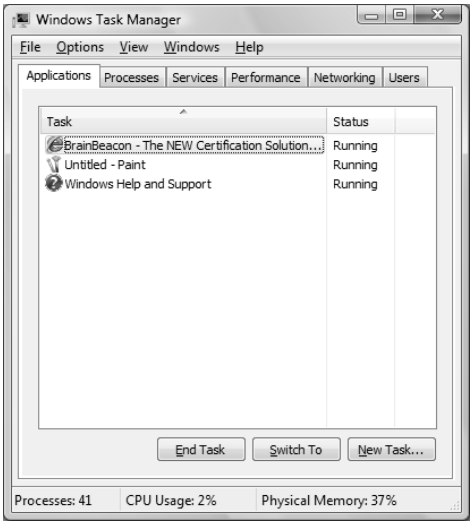
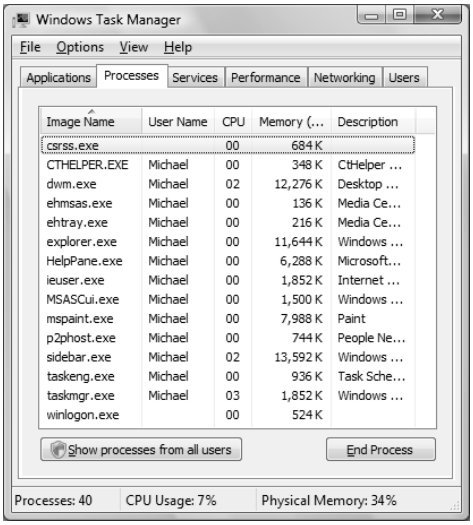


FIGURE 11.20 Task Manager, Processes tab



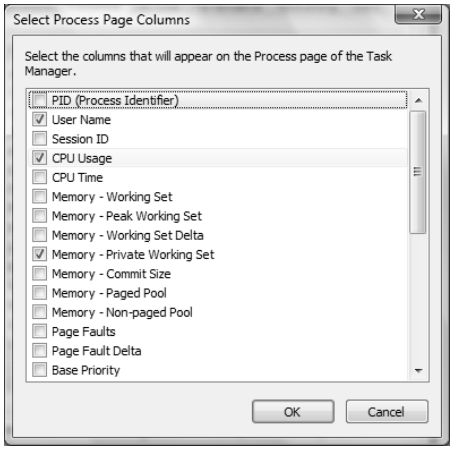
From the Processes tab, you can organize the listing and control processes as follows:

- To organize the processes, click the column headings. For example, if you click the CPU column, the listing will start with the processes that use the most CPU resources. If you click the CPU column a second time, the listing will be reversed so that the processes that use the least CPU resources are listed first.
- To manage a process, right-click it and choose an option from the context menu. You can choose to end the process, end the process tree, debug the process, specify virtualization, create a dump file, or set the priority of the process (to Realtime, High, Above Normal, Normal, Below Normal, or Low). If your computer has multiple processors installed, you can also set processor affinity (the process of associating a specific process with a specific processor) for a process.
- To customize the counters that are listed, select View ➢ Select Columns. This brings up the Select Columns dialog box, shown in Figure 11.21, where you can select the information that you want to see listed on the Processes tab.

By default, only your processes are shown. To display processes from all users, including SYSTEM, LOCAL SERVICE, and NETWORK SERVICE, click Show Processes from All Users.

In the following subsections you will learn how to stop processes and manage process priority.

FIGURE 11.21 Selecting information for the Task Manager's Processes tab



Stopping Processes

You may need to stop a process that isn't executing properly. To stop a specific process, select the process you want to stop in the Task Manager's Processes tab and click the End Process button. Task Manager displays a Warning dialog box. Click the End Process button to terminate the process.

If you right-click a process, you can end the specific process or you can use the option End Process Tree. The End Process Tree option ends all processes that have been created either directly or indirectly by the process.

Some of the common processes that can be managed through Task Manager are listed in Table 11.1.

TABLE 11.1 Common Processes

Process	Description
System Idle Process	A process that runs when the processor is not executing any other threads
`smss.exe`	Session Manager subsystem
`csrss.exe`	Client-server runtime server service
`mmc.exe`	Microsoft Management Console program (used to track resources used by MMC snap-ins such as Reliability and Performance Monitor)
`explorer.exe`	Windows Explorer interface

Managing Process Priority

You can manage process priority through the Task Manager utility. To change the priority of a process that is already running, use the Processes tab of Task Manager. Right-click the process you want to manage and select Set Priority from the context menu. You can select from Realtime, High, Above Normal, Normal, Below Normal, and Low priorities. As you might expect, applications launch at Normal priority by default.

Running a process-intensive application in the RealTime priority class can significantly impact performance.

In Exercise 11.6, you will set the priority for a process.

EXERCISE 11.6

Setting a Process Priority

1. Right-click an empty space on your taskbar and select Task Manager from the context menu.
2. On the Applications tab, click the New Task button.
3. In the Create a New Task dialog box, type **CALC** and click OK.

EXERCISE 11.6 *(continued)*

4. Click the Processes tab. Right-click `calc.exe` and select Set Priority, then Low. In the Task Manager Warning dialog box, click the Change Priority button to continue.
5. Right-click `calc.exe` and select End Process. In the Task Manager Warning dialog box, click the End Process button.

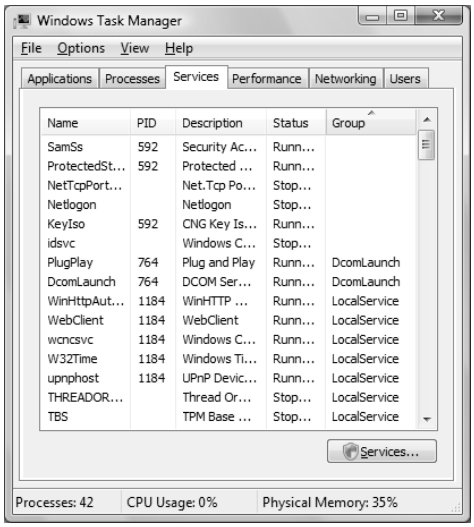
Managing Services

The Services tab of the Task Manager dialog box, shown in Figure 11.22, lists all the services that can run on the computer. For each service, you will see the Name (the name of the service), the PID (the associated process identifier), Description (a description of the service, Status (whether a process is Running or Stopped), and Group (the service group).

To start a stopped service, click the service and select Start Service. To stop a running service, click the service and select Stop Service. You can also open the Services tool by clicking the Services button. The Services tool allows you to specify whether a process starts automatically, automatically with a delayed start, manually, or is disabled.

We describe the Services tool in detail in Chapter 3.

FIGURE 11.22 Task Manager, Services tab



Managing Performance Tasks

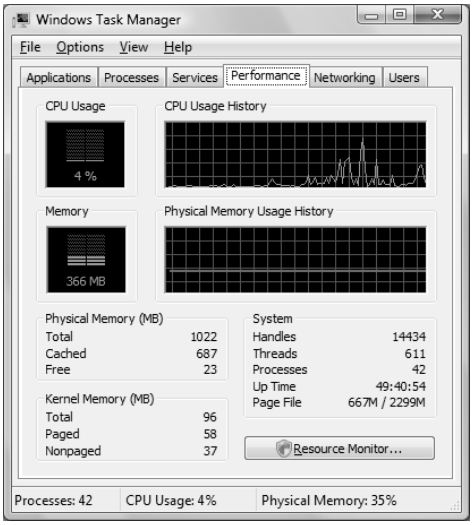
The Performance tab of the Task Manager dialog box, shown in Figure 11.23, provides an overview of your computer's CPU and memory usage. This is similar to the information tracked by Reliability and Performance Monitor.

The Performance tab shows the following information:

- CPU Usage, in real time and in a history graph
- Memory Usage, in real time and in a history graph
- Physical Memory statistics
- Kernel Memory statistics
- System totals for handles, threads, processes, uptime, and the pagefile

Clicking Resource Monitor will launch the Resource Overview portion of Reliability and Performance Monitor.

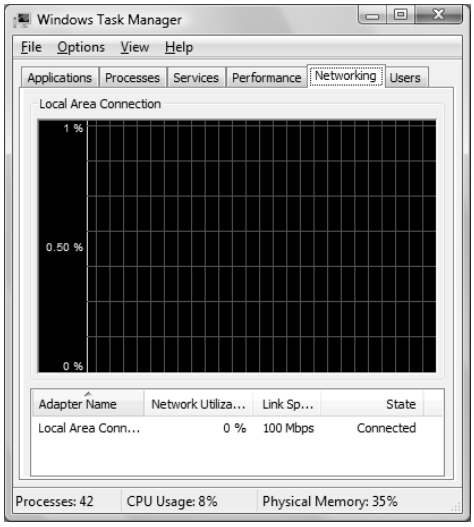
FIGURE 11.23 Task Manager, Performance tab



Managing Networking Tasks

The Networking tab of the Task Manager dialog box, shown in Figure 11.24, provides an overview of your networking usage. Statistics for each adapter are displayed at the bottom of the dialog box.

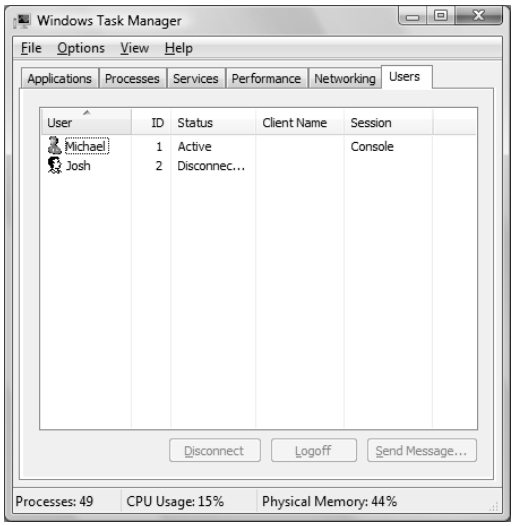
FIGURE 11.24 Task Manager, Networking tab



Managing Users

The Users tab of the Task Manager dialog box, shown in Figure 11.25, shows the active and disconnected users on your computer. For each user, you will see the User (the name of the user), the ID (the current user ID), Status (whether Active or Disconnected), Client Name, and Session (whether the user is connected via the console session or by another method, such as Remote Desktop).

FIGURE 11.25 Task Manager, Users tab



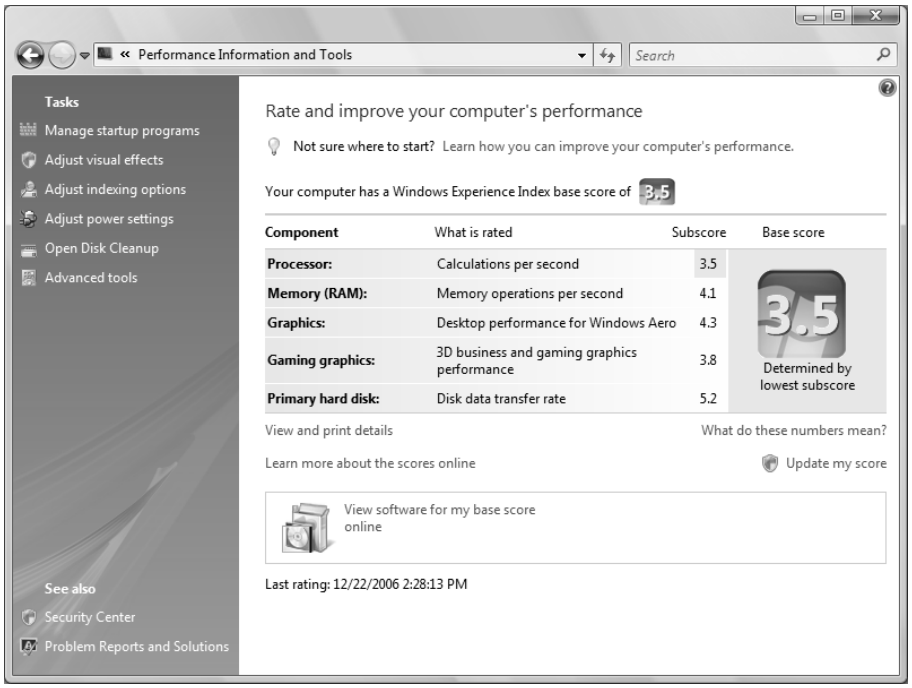
Windows Vista is limited to one concurrent user session. Therefore, only one session will be active at a time.

To send a message to a user, select the user and click the Send Message button. To connect to a user session, right-click the user and select Connect. To disconnect a user session, select the user and click the Disconnect button. To log off a user, select the user and click the Logoff button.

Performance Information and Tools

If you enjoy seeing how well your computer performs by running benchmarking applications that provide a score rating, then you will love *Performance Information and Tools*, shown in Figure 11.26. This utility provides you with a numerical score that lets you know how well your system performs. To launch Performance Information and Tools, click Start ➢ Control Panel ➢ System and Maintenance ➢ Performance Information and Tools.

FIGURE 11.26 Performance Information and Tools



The main pane reveals a calculated score, called the *Windows Experience Index*. The Windows Experience Index base score is calculated by taking the lowest subscore among five rated components:

- Processor, based on calculations per second
- Memory (RAM), based on memory operations per second
- Graphics, based on Windows Aero performance
- Gaming Graphics, based on 3D graphics performance
- Primary Hard Disk, based on disk transfer rate

A computer with a base score of 1 or 2 will be able to perform only the most basic tasks. A base score of 3 indicates that a computer can run Windows Aero and all but the most advanced Windows Vista features. A base score of 4 or 5 should be able to run all Windows Vista features, as well as play graphically intensive 3D games. At the time Windows Vista was released, computers with a base score of 5 were among the best-performing computers available. As technology improves, the base scores will begin to rise so that eventually computers may need a base score of 10 or 15 to play newer games or run resource-intensive applications.

Each component subscore determines how well each individual component performs. Because the base score is equal to the lowest component subscore, the Windows Experience Index base score should give you an overview of how well your computer should run applications. This enables application developers to give their applications a numerical rating so that consumers can easily figure out if the application will run well on their computer. If an application requires a higher base score than your computer has, it might be time to upgrade your hardware. After you install new hardware, you can select Update My Score to have Windows Vista recalculate your Windows Experience Index base score.

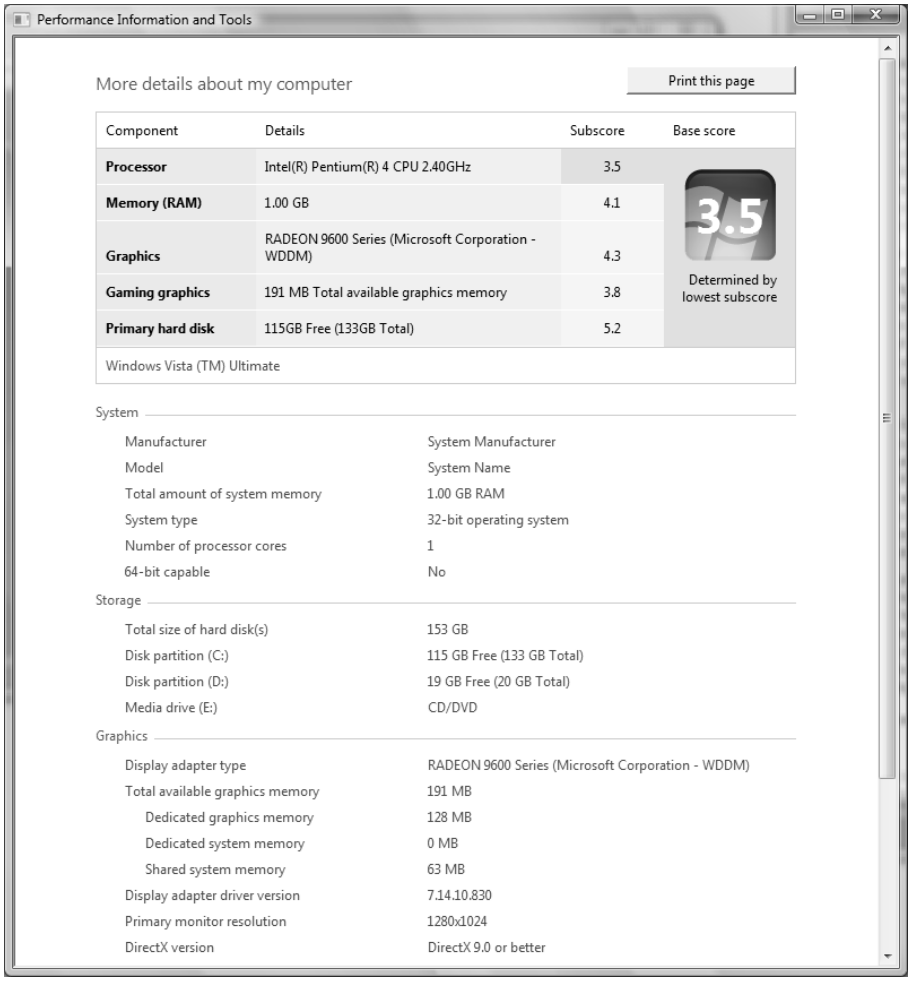
You can view and purchase software that will run on your computer by clicking View Software for My Base Score Online, which will take you to the Windows Marketplace. Clicking View and Print Details will enable you to view details about your computer's hardware components, as shown in Figure 11.27.

The left pane of Performance Information and Tools contains useful links to help you improve the performance of your computer. Clicking Manage Startup Programs will launch the Software Explorer component of Windows Defender, where you can remove, disable, or enable startup programs and end running processes. Clicking Adjust Visual Effects will bring up the Visual Effects tab of the Performance Options dialog box, which is used for configuring how Windows will graphically display windows, menu items, and icons. Clicking Adjust Indexing Options will launch Indexing Options, which can improve the speed of searching files on your computer. Clicking Adjust Power Settings will launch Power Options, which is used to adjust your power plan. Clicking Open Disk Cleanup will launch Disk Cleanup Options so that you can clean up unnecessary files on your hard disk. Finally, clicking Advanced Tools will launch a list of tools you can use to further improve your computer's performance, including the following:

- View Performance Details in Event Log
- Open Reliability and Performance Monitor

- Open Task Manager
- View Advanced System Details in System Information
- Adjust the Appearance and Performance of Windows
- Open Disk Defragmenter
- Generate a System Health Report

FIGURE 11.27 Performance Information and Tools—More Details About My Computer



Using the System Tool in Control Panel

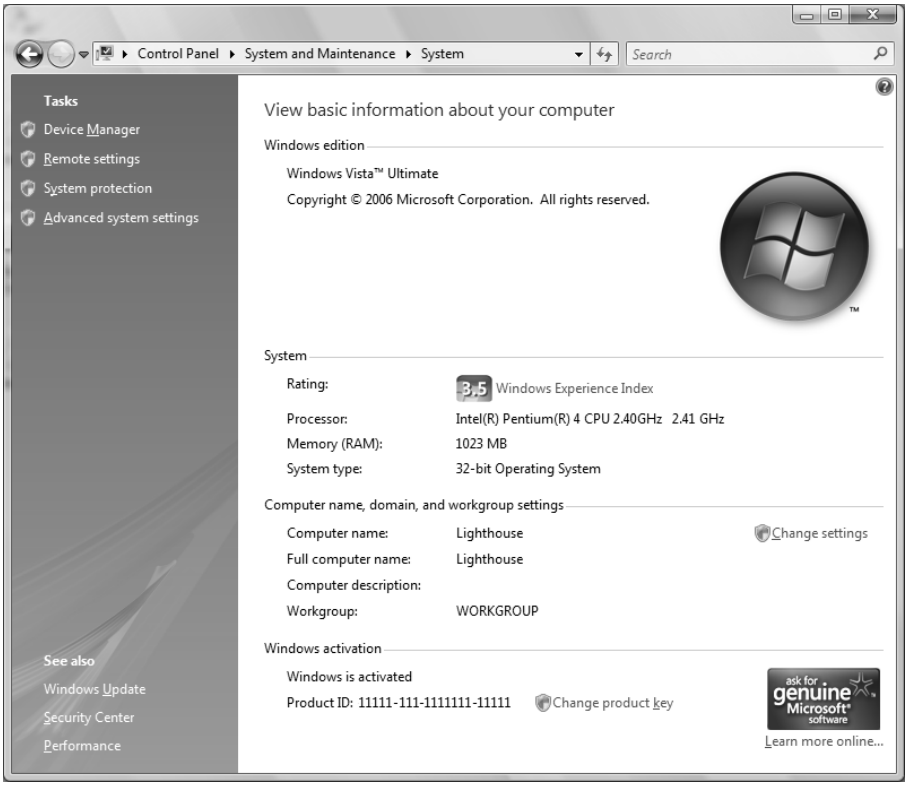
The *System tool* in Control Panel can be used to manage performance options for your computer. To access the System tool, select Start ➢ Control Panel ➢ System and Maintenance ➢ System. Figure 11.28 shows the System dialog box.

The top portion of the window shows the edition of Windows Vista that is currently installed. Below this section is the System section, which specifies the following information:

- Windows Experience Index
- Processor speed and quantity
- Physical memory
- System type (32-bit or 64-bit)

Clicking Windows Experience Index will launch Performance Information and Tools.

FIGURE 11.28 System dialog box



We discussed Performance Information and Tools earlier in this chapter.

The next section displays the computer name, description, and workgroup or domain. Clicking Change Settings will bring up the Computer Name tab of the System Properties dialog box, shown in Figure 11.29, where you can change the computer name and description, or join the computer to a domain or workgroup.

The final section displays the status of Windows activation and the product ID. Clicking Change Product Key will launch the Windows Activation Client, shown in Figure 11.30, where you can change your product key. The product key can usually be found on the computer case or on the Windows Vista installation disc holder.

The left pane contains four links:

- Device Manager
- Remote Settings
- System Protection
- Advanced System Settings

Clicking Device Manager launches Device Manager. You can also access Device Manager by clicking Start ➢ Control Panel ➢ System and Maintenance ➢ Device Manager.

FIGURE 11.29 System Properties, Computer Name tab

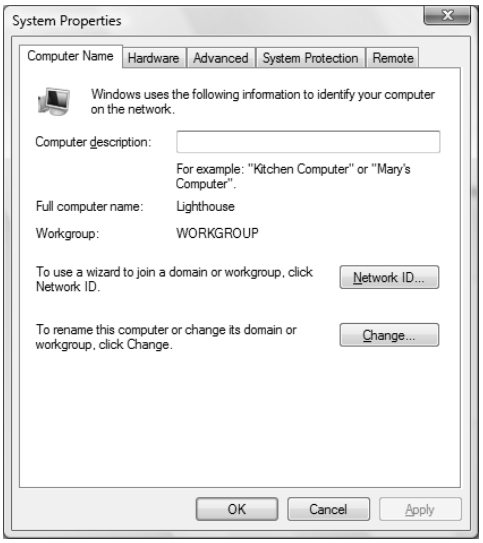
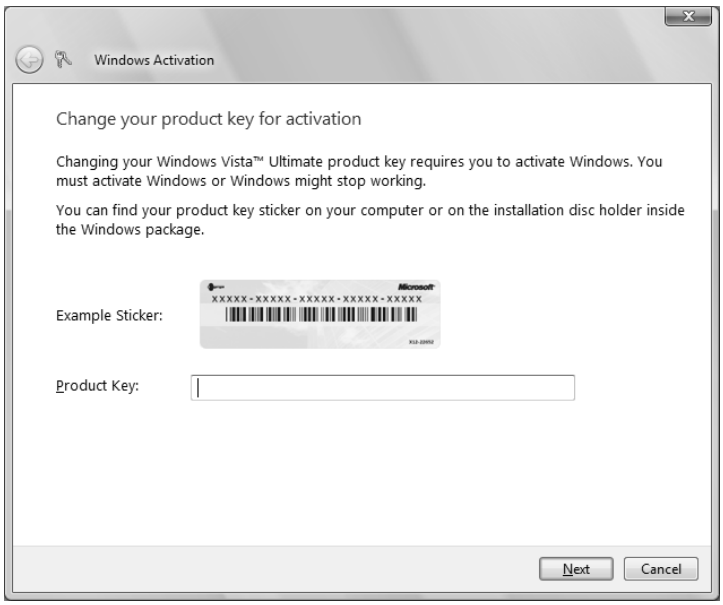


FIGURE 11.30 Windows Activation Client



Clicking Remote Settings will bring up the Remote tab of the System Properties dialog box, where you can configure Remote Assistance and Remote Desktop properties.

Clicking System Protection will bring up the System Protection tab of the System Properties dialog box, where you can configure restore points.

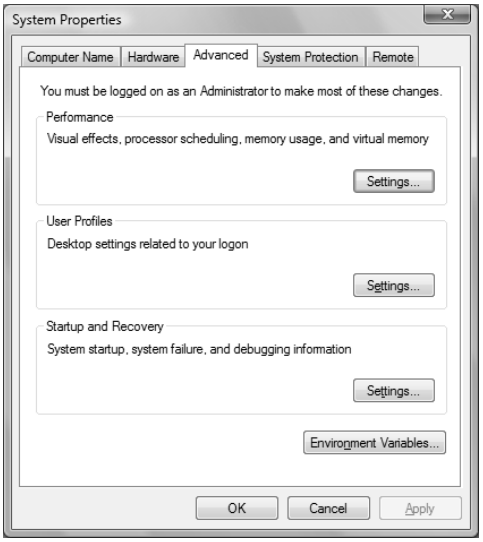
Clicking Advanced System Settings will bring up the Advanced tab of the System Properties dialog box, where you can configure advanced settings related to performance, profiles, and startup options.

Device Manager is covered in detail in Chapter 3. Remote Desktop, Remote Assistance, and System Protection are covered later in this chapter.

Advanced System Settings

The Advanced tab of the System Properties dialog box is where you can configure settings such as visual effects, processor scheduling, memory usage, virtual memory, user profiles, startup and recovery settings, and environment variables. To modify these settings, click Start ➢ Control Panel ➢ System and Maintenance ➢ System, then click Advanced System Settings in the left pane. The System Properties dialog box in Figure 11.31 will be displayed.

FIGURE 11.31 System Properties, Advanced tab



In order to access Advanced System Settings, you must be logged onto the local computer with administrative rights.

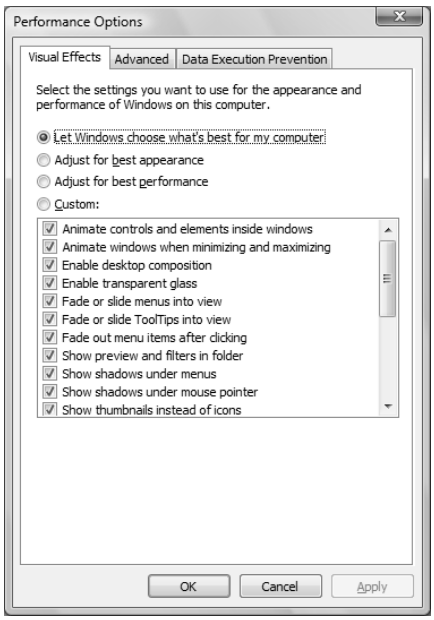
Performance

The first section is for performance-related options. Clicking Settings in this section will bring up the Performance Options dialog box. The first tab is the Visual Effects tab, as shown in Figure 11.32. This tab is used for configuring how Windows will graphically display windows, menu items, and icons. The selections for visual effect settings include the following:

- Let Windows Choose What's Best for My Computer
- Adjust for Best Appearance
- Adjust for Best Performance
- Custom

If many graphical details and effects are slowing down your computer, you should deselect some of the options under Custom, or you should select Adjust for Best Performance. Selecting Adjust for Best Performance sacrifices some visual features for the benefit of processor speed.

FIGURE 11.32 The Visual Effects tab of the Performance Options dialog box



If you click the Advanced tab, you will see the dialog box shown in Figure 11.33. On the Advanced tab, you can configure these options:

- Processor Scheduling, which allows you to optimize the processor time for running programs or background services
- Virtual Memory, which is used to configure the paging file

If you click the Change button in the Virtual Memory section of the Advanced tab, the Virtual Memory dialog box will appear, as shown in Figure 11.34. You can optimize the paging file, `pagefile.sys`, by moving it from the drive that contains the system partition or by splitting it over multiple disk I/O channels.

The last tab is for *Data Execution Prevention (DEP)*. DEP, which was introduced with Windows XP Service Pack 2, helps prevent damage to the operating system and applications from viruses and security threats. It does this by monitoring how programs access and use system memory. If DEP notices an application that accesses memory incorrectly, DEP will close the application and notify you.

Some CPUs include hardware-based DEP functionality. However, for those computers that do not have a processor with DEP functionality, Windows Vista includes software-based DEP.

On the Data Execution Prevention tab, shown in Figure 11.35, you can choose to enable DEP only for essential Windows programs and services, or you can choose to enable DEP for all programs and services except for those you specify in an exclusion list.

FIGURE 11.33 The Advanced tab of the Performance Options dialog box

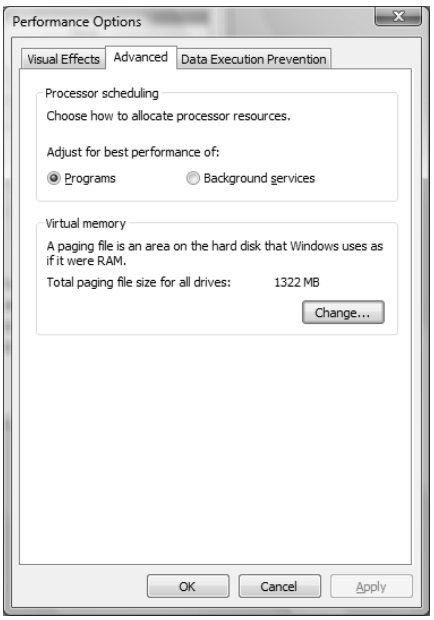


FIGURE 11.34 Virtual Memory dialog box

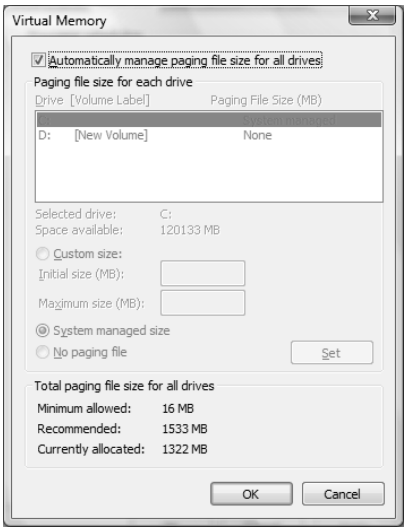
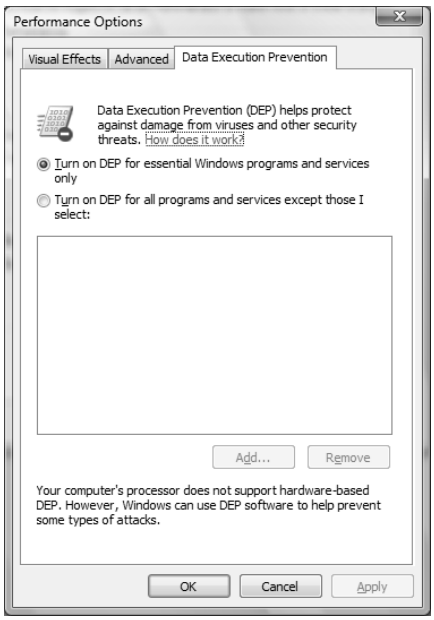


FIGURE 11.35 The Data Execution Prevention tab of the Performance Options dialog box



User Profiles

The next section is for User Profiles. Clicking the Settings button in this section will bring up the User Profiles dialog box, as shown in Figure 11.36. Local users who are set up on the computer will be listed here. You can click the Change Type button to change whether the user has a local or a roaming profile. The Delete button is used to delete a local profile. The Copy To button is used to copy a profile to another location.

We cover user profiles in detail in Chapter 5, "Configuring Users and Groups."

Startup and Recovery

The final section is for startup and recovery options. Clicking the Settings button in this section will bring up the Startup and Recovery dialog box, as shown in Figure 11.37. The Startup and Recovery options (see Table 11.2) are used to specify the default operating system that is loaded and to specify which action should be taken in the event of system failure.

FIGURE 11.36 User Profiles dialog box

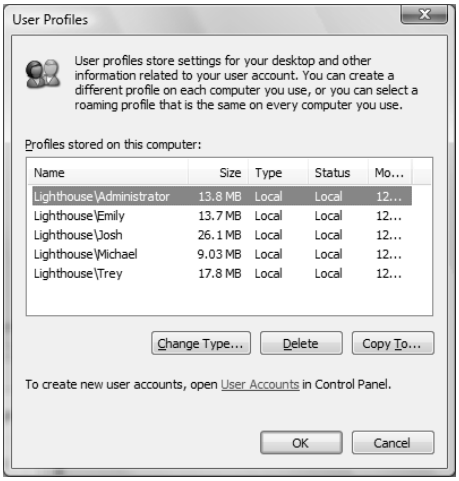


FIGURE 11.37 The Startup and Recovery dialog box

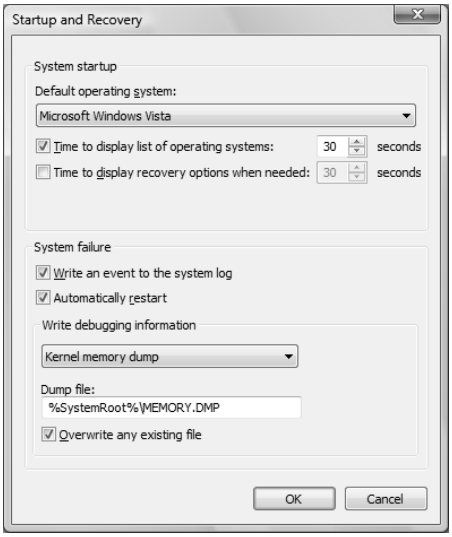


TABLE 11.2 Startup and Recovery Options

Option	Description
Default Operating System	Specifies the operating system that is loaded by default if no selection is made from the operating system selection menu (if your computer dual-boots or multiboots and an operating system selection menu appears during boot-up). The default setting for this option is Microsoft Windows Vista.
Time to Display List of Operating Systems	Specifies how long the operating system selection menu is available before the default selection is loaded (if your computer dual-boots or multiboots and an operating system selection menu appears during boot-up). The default setting for this option is 30 seconds.
Time to Display Recovery Options When Needed	Specifies how long the advanced recovery options selection menu will be displayed if the computer cannot start properly. The default setting for this option is 30 seconds.
Write an Event to the System Log	Specifies that an entry be made in the System log any time a system failure occurs. This option is enabled by default, which allows you to track system failures.
Automatically Restart	Specifies that the computer will automatically reboot in the event of a system failure. This option is enabled by default, so the system restarts after a failure without intervention. You would disable this option if you wanted to see the blue screen for analysis.
Write Debugging Information	Specifies that debugging information (a memory dump) be written to a file. You can choose not to create a dump file or to create a small memory dump (64KB) file, a kernel memory dump file, or a complete memory dump file. Complete memory dump files require free disk space equivalent to your memory and a pagefile that is at least as large as your memory with an extra 2MB. The default setting is to write debugging information to a kernel memory dump file.
Dump File	Specifies the location and name of the dump file. The default setting is %SystemRoot%\MEMORY.DMP.
Overwrite Any Existing File	If you create dump files, this option allows you to create a new dump file that overwrites the old dump file or to keep all dump files each time a system failure occurs.

In Exercise 11.7, you will access the Startup and Recovery options and make changes to the settings.

EXERCISE 11.7

Using Startup and Recovery Options

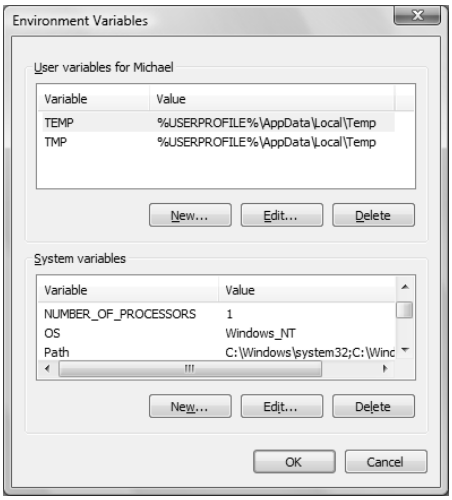
1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ System, then click Advanced System Settings in the left pane. The Advanced tab of the System Properties dialog box will be displayed.
2. Click Settings next to Startup and Recovery. The Startup and Recovery dialog box will be displayed.
3. Change the setting for Display List of Operating Systems from 30 seconds to 10 seconds.
4. In the Write Debugging Information section, choose (None) from the drop-down list.
5. Click OK to close the Startup and Recovery dialog box, then click OK to close the System Properties dialog box.

Environment Variables

Clicking the Environment Variables button at the bottom of the Advanced tab of the System Properties dialog box brings up the Environment Variables dialog box, shown in Figure 11.38. Environment variables are used to configure the following:

- User-specific variables, such as the location of the user's TEMP directory
- System-specific variables, such as the number of processors, processor architecture, PATH statement, system TEMP directory, and the OS directory

FIGURE 11.38 Environment Variables dialog box



Using System Configuration

The *System Configuration* utility is used to help you view and troubleshoot how Windows Vista starts and what programs and services launch at startup. You may recognize this utility as `msconfig.exe`. To launch this utility, run `msconfig.exe` from the command prompt.

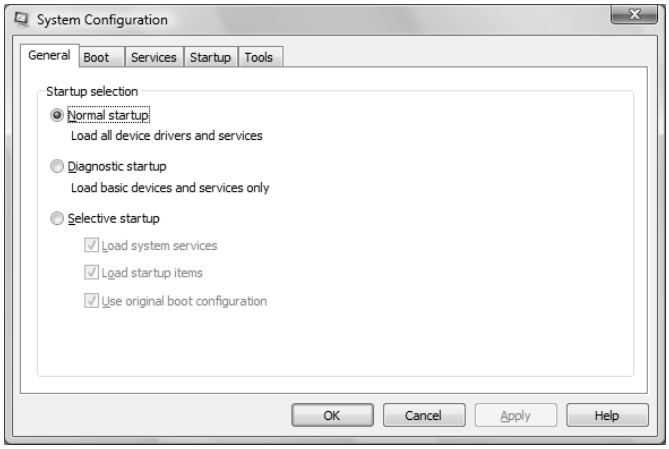
The General tab, shown in Figure 11.39, is used to specify startup options. You can choose from the following three startup options:

- Normal Startup, which loads all device drivers and services
- Diagnostic Startup, which loads basic services and drivers
- Selective Startup, from which you can choose whether or not to load system services, load startup items, and use the original boot configuration

The Boot tab, shown in Figure 11.40, is used to configure whether Windows Vista boots in Safe Mode, runs an Active Directory repair, boots to a graphical user interface (GUI), logs boot information, boots in VGA mode, and displays driver names while Windows Vista boots. Selecting any of the options on this screen will change the settings on the General tab; conversely, selecting Normal Startup on the General tab will clear the settings on the Boot tab.

The Services tab, shown in Figure 11.41, is used to show Windows Vista services and indicates which services are running. You can deselect services on this tab so that they do not launch at startup. Selecting any of the services on this screen will change the settings on the General tab; conversely, selecting Normal Startup on the General tab will clear the settings on the Services tab.

FIGURE 11.39 System Configuration, General tab



The Startup tab, shown in Figure 11.42, shows applications that start when Windows Vista starts. You can deselect applications on this tab so that they do not launch at startup. If you've read through the previous two paragraphs, you can probably guess that selecting any of the services on this screen will change the settings on the General tab, and selecting Normal Startup on the General tab will clear the settings on the Startup tab.

FIGURE 11.40 System Configuration, Boot tab

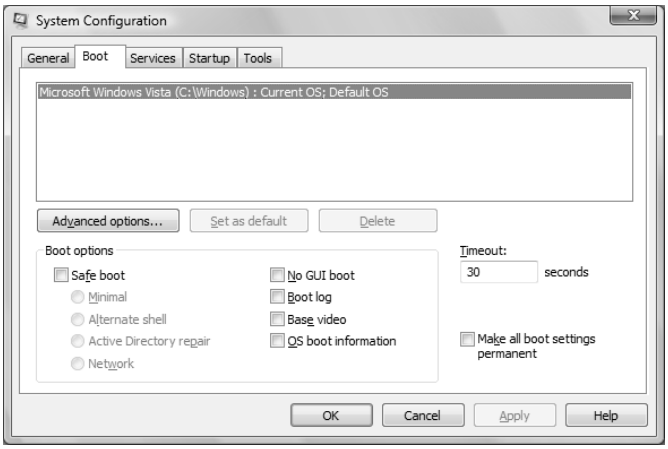


FIGURE 11.41 System Configuration, Services tab

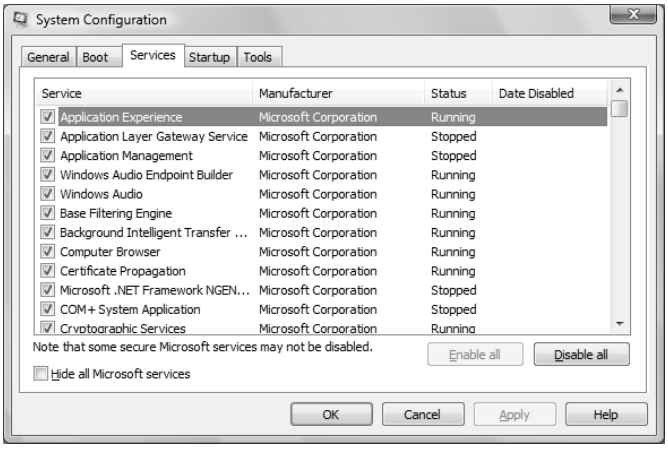
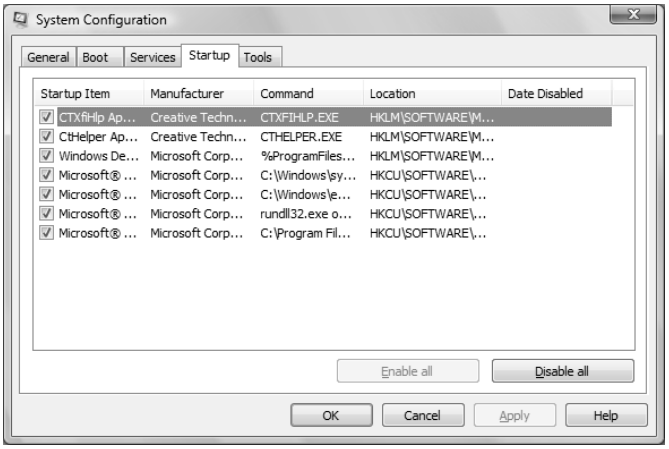


FIGURE 11.42 System Configuration, Startup tab

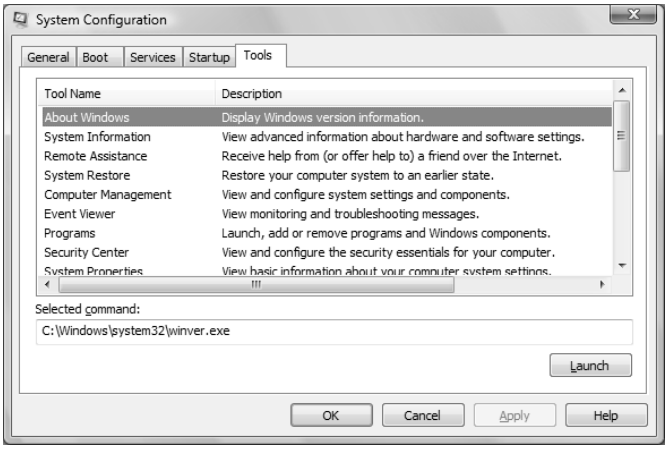


The Tools tab, shown in Figure 11.43, is new to Windows Vista. This tab shows tools that you can launch from System Configuration. Simply click the tool name and click Launch to launch the tool. The following tools can be launched from this tab:

- About Windows
- System Information
- Remote Assistance
- System Restore
- Computer Management
- Event Viewer
- Programs
- Security Center
- System Properties
- Internet Options
- Internet Protocol Configuration
- Performance Monitor
- Task Manager
- Disable UAC
- Enable UAC
- Command Prompt
- Registry Editor

In Exercise 11.8, you will access System Configuration and configure Windows Vista to boot in Safe Mode running only basic services.

FIGURE 11.43 System Configuration, Tools tab



EXERCISE 11.8

Using System Configuration

1. Select Start ➢ Run, type **msconfig** in the Run dialog box, and click OK. The System Configuration utility will be displayed.
2. Click the Boot tab.
3. Click the check box next to Safe Boot, then select the Network radio button. Click Apply to save your changes.
4. Click the General tab. Notice that Selective Startup is enabled with Load System Services and Load Startup Items checked.
5. If you want to see Windows boot into Safe Mode, exit the System Configuration utility. You will be prompted to restart your computer or to exit without restarting. Select Restart.
6. After you have finished testing, select the Normal Startup radio button on the General tab, then click Apply to save your changes.

Using Task Scheduler

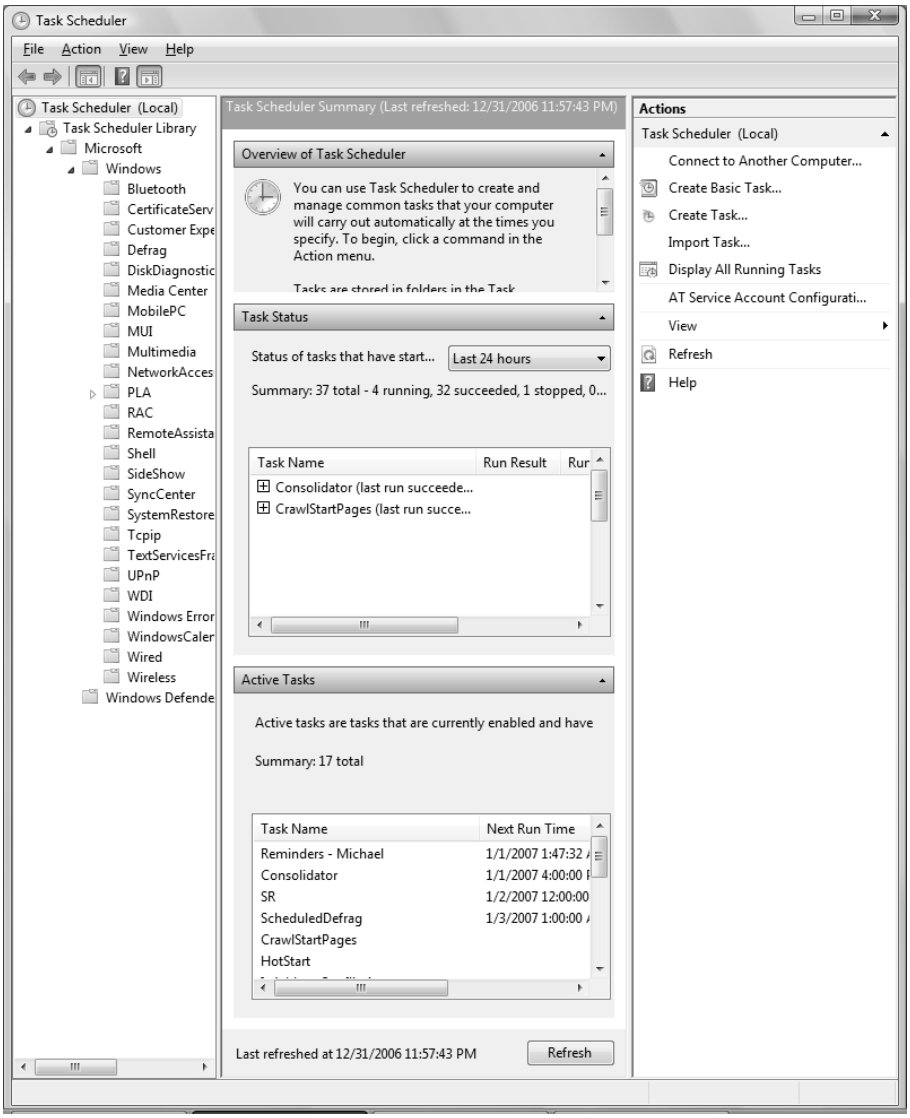
Task Scheduler has been completely overhauled for Windows Vista. Task Scheduler, shown in Figure 11.44, is a utility that allows you to schedule actions to occur at specified intervals. You can set any of your Windows programs to run automatically at a specific time and at a set

interval, such as daily, weekly, or monthly. For example, you might schedule an application to run daily at 2:00 AM.

Actions can be performed at the following times, called *triggers*:

- Daily, or once every number of days (such as once every three days)

FIGURE 11.44 Task Scheduler



- Weekly, or on certain days of the week, or every number of weeks (such as every four weeks on Monday)
- Monthly, or on selected days of the month, or only on selected months
- One time only
- At startup
- At logon
- When a specific event is logged

When a trigger is activated, Task Scheduler can perform the following *actions*:

- Start a program or script
- Display a message
- Send an e-mail

Windows Vista makes heavy use of Task Scheduler. In fact, Windows Vista comes with several predefined tasks that you can choose from. These tasks are sorted by category into task folders. For example, the Defrag task folder contains two tasks: ManualDefrag and ScheduledDefrag. You can also create your own task folders to help you manage your scheduled tasks.

Task Scheduler also allows you to run tasks manually by selecting the task and clicking Run in the righthand pane. Selecting a task and clicking Disable will disable a task. You can also export and import tasks.

If you are using Task Scheduler and your jobs are not running properly, make sure that the Task Scheduler service is running and is configured to start automatically. You should also ensure that the user who is configured to run the scheduled task has sufficient permissions to run the task.

In Exercise 11.9, we will create a new scheduled task.

After you create a task, it will be added to your Task Scheduler Library.

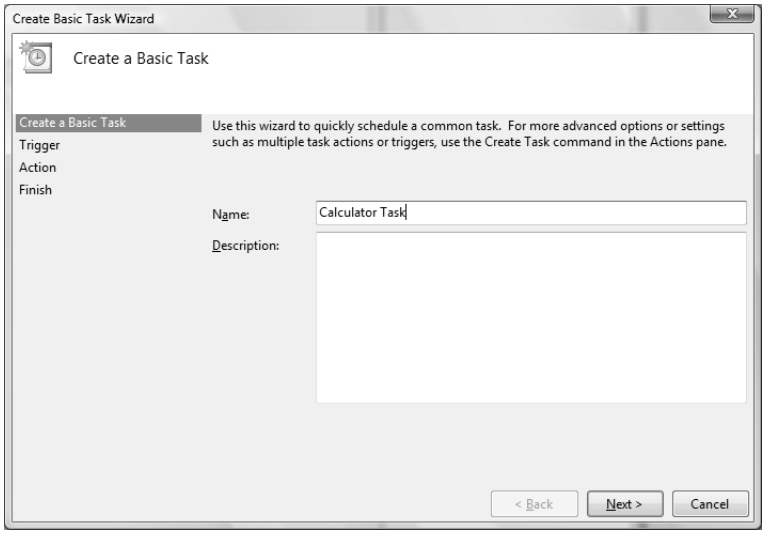
EXERCISE 11.9

Creating a New Scheduled Task

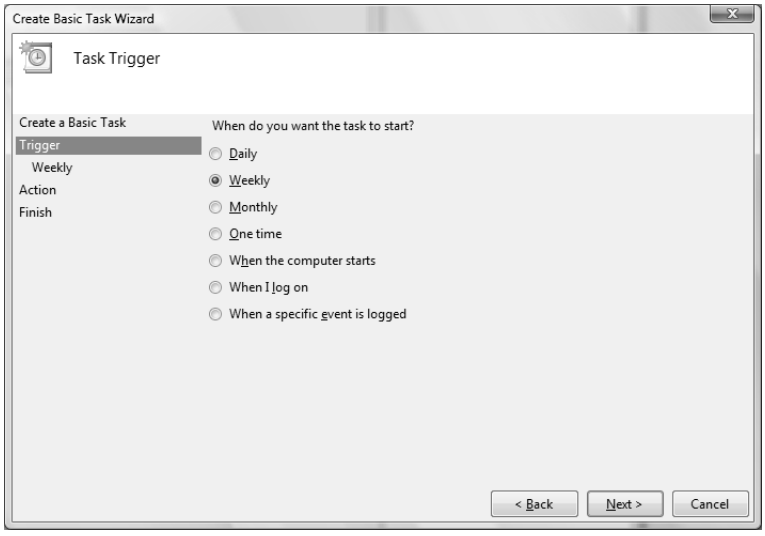
1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools ➢ Task Scheduler.
2. In the right pane of the Task Scheduler window, select Create Basic Task.

EXERCISE 11.9 *(continued)*

3. The Create Basic Task Wizard appears. Type a name for your task and a description, then click Next.

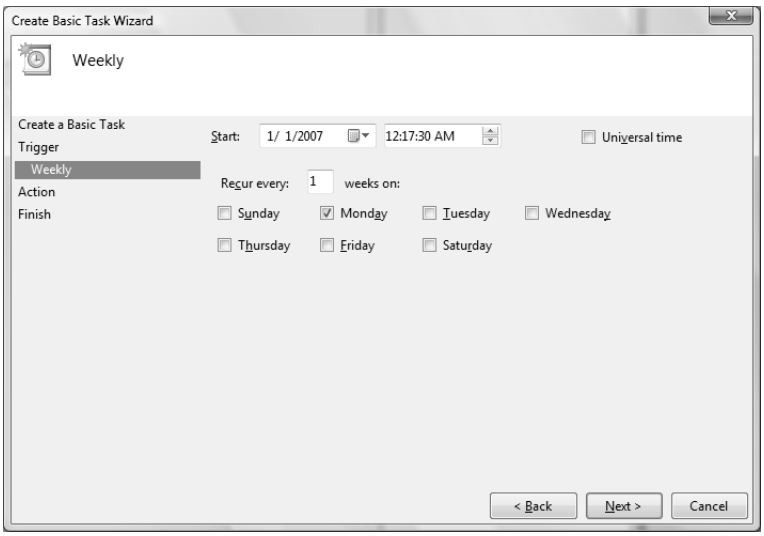


4. You are prompted to select a trigger. Select how often you want the action to occur. In this exercise, we will select Weekly. Click Next to continue.

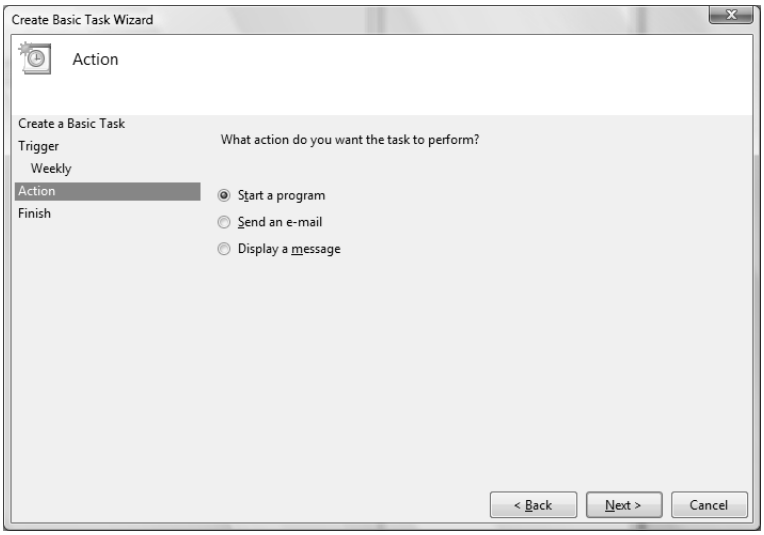


EXERCISE 11.9 *(continued)*

5. If you selected Daily, Weekly, Monthly, One Time, or When a Specific Event Is Logged, you will be prompted for more information. For this example, since we selected Weekly, we will specify that the action should occur every Monday. Click Next to continue.

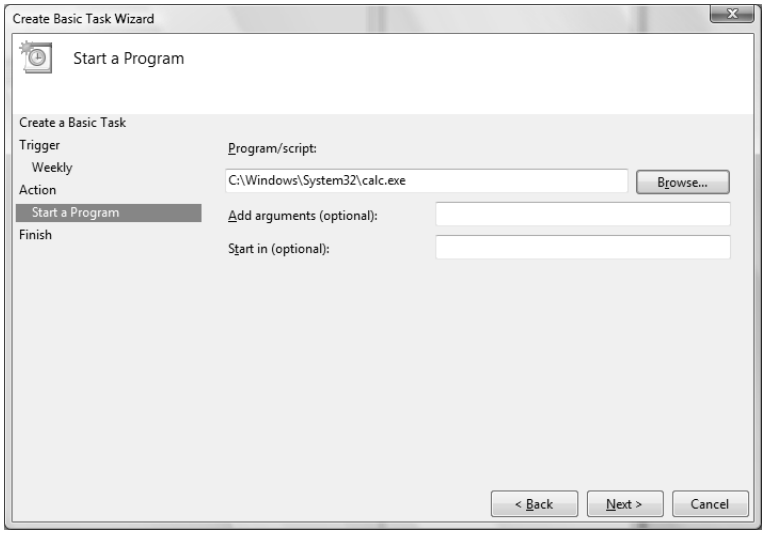


6. You are prompted to select an action. In this exercise, we will select Start a Program. Click Next to continue.

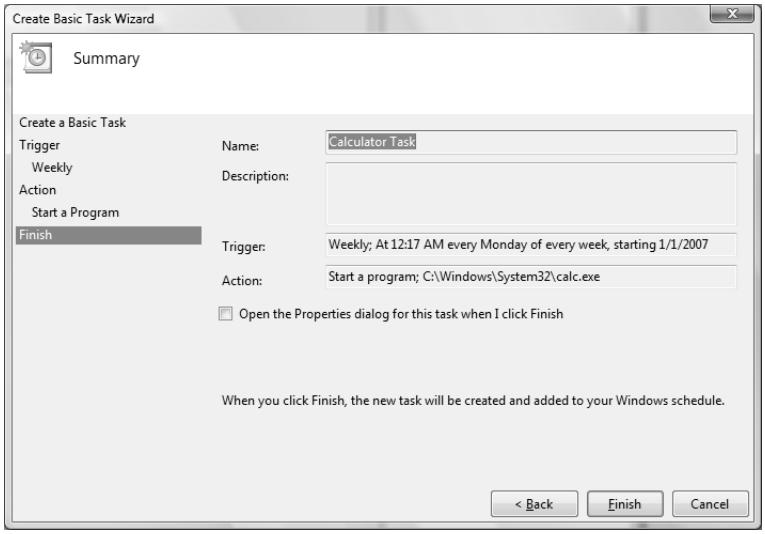


EXERCISE 11.9 *(continued)*

7. You are prompted for more information regarding your action, whether it be the program or script to launch, the e-mail to send and server to use, or the message to display. Since we selected Start a Program, we will browse for the Calculator application at `C:\windows\system32\calc.exe`. Click Next to continue.



8. The final dialog box shows your selections for the scheduled task. If this information is correct, click the Finish button.



Managing Scheduled Task Properties

You can manage a scheduled task through its properties dialog box. To access this dialog box, right-click the task you wish to manage and choose Properties from the context menu.

The scheduled task's properties dialog box has six tabs:

- General
- Triggers
- Actions
- Conditions
- Settings
- History

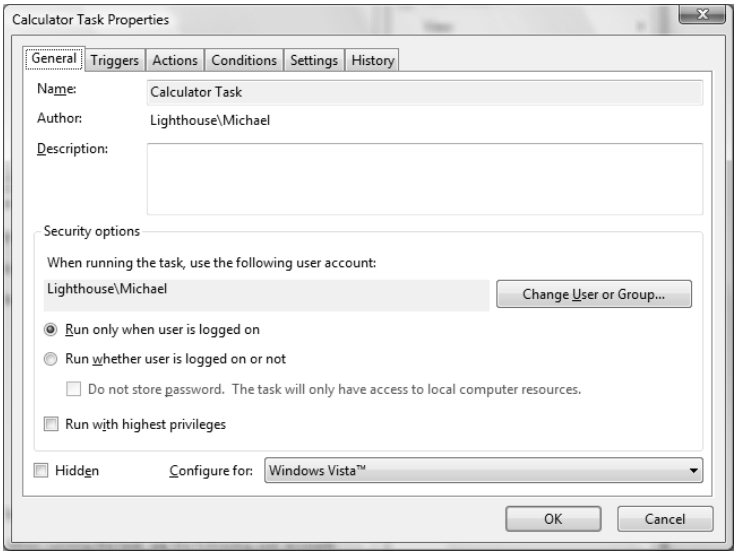
These options are described in the following sections.

General Properties

On the General tab, shown in Figure 11.45, you can configure the following options:

- The description of the task
- The username or group to be used to run the specified task
- Whether the task is run when the user is logged off
- Whether the task is hidden

FIGURE 11.45 The Task properties for the scheduled task



Triggers Properties

The Triggers tab, shown in Figure 11.46, shows the schedule configured for the task. You can click Edit to edit the trigger, which will bring up the Edit Trigger dialog box, shown in Figure 11.47. You can also click New to create a new trigger, or click Delete to delete an existing trigger.

Actions Properties

The Actions tab (Figure 11.48) shows the action that is configured for the task. You can click Edit to edit the action, which will bring up the Edit Action dialog box, shown in Figure 11.49. You can also click New to create a new action, or click Delete to delete an existing action.

Conditions Properties

The Conditions tab (Figure 11.50) shows the conditions associated with the task. The options in the Idle section are useful if the computer must be idle when the task is run. You can specify how long the computer must be idle before the task begins and whether the task should be stopped if the computer ceases to be idle.

The options in the Power section are applicable when the computer on which the task runs is battery powered. You can specify that the task should not start if the computer is running from batteries and choose to stop the task if battery mode begins. You can also select whether to wake the computer in order to run the task.

The option in the Network section defines whether the task starts when a particular network connection is available.

FIGURE 11.46 The Triggers properties for the scheduled task

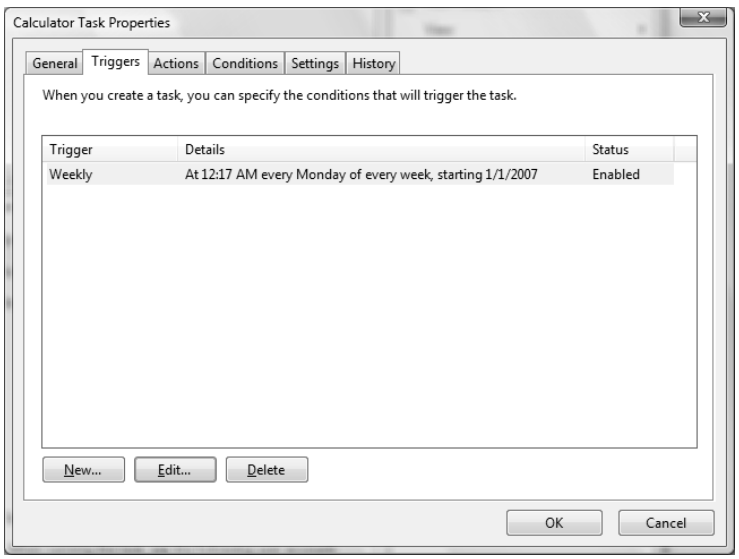


FIGURE 11.47 The Edit Trigger dialog box

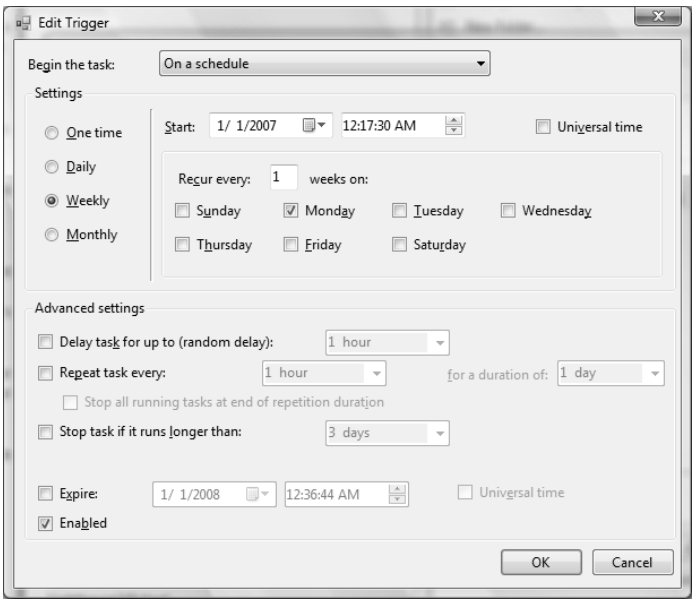


FIGURE 11.48 The Actions properties for the scheduled task

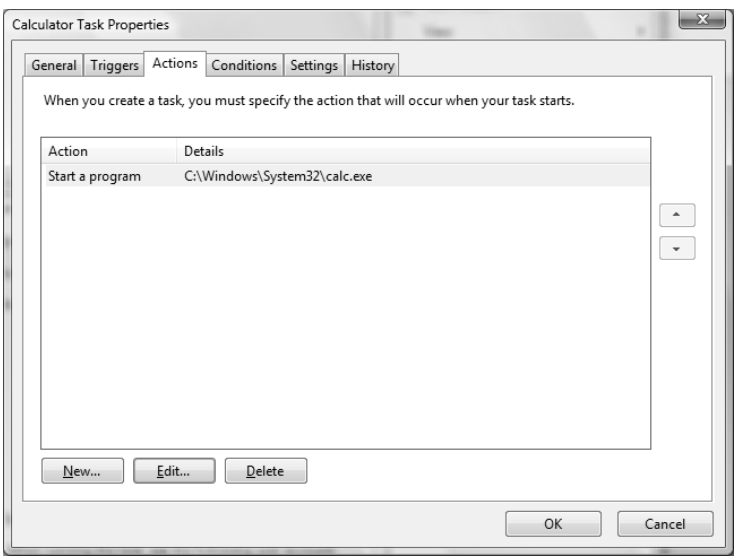


FIGURE 11.49 The Edit Action dialog box

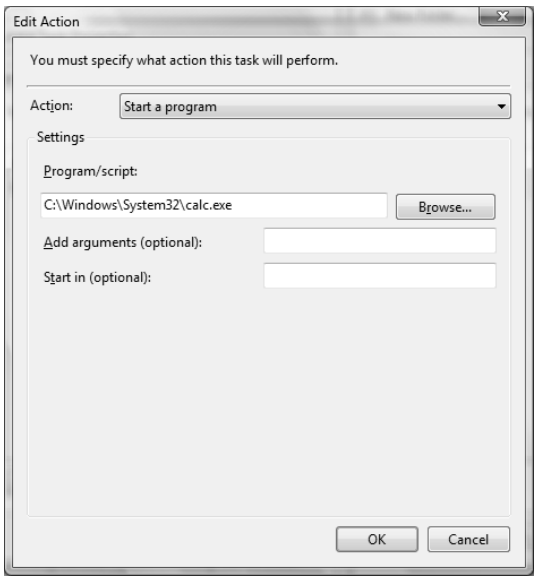
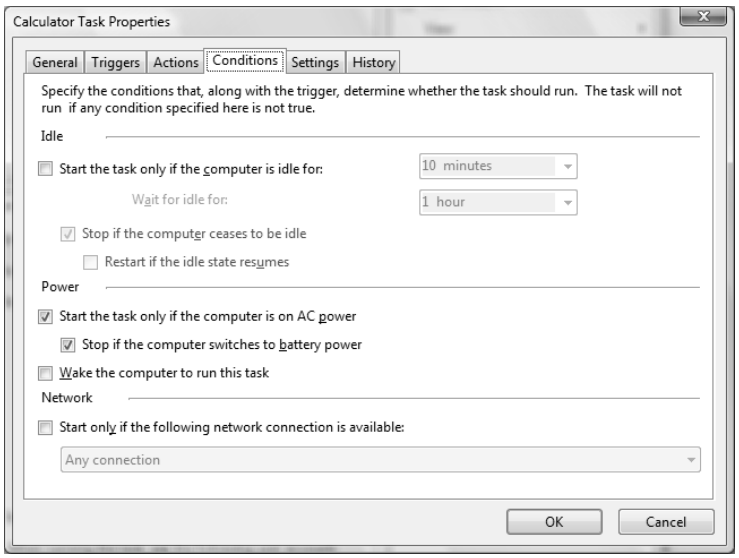


FIGURE 11.50 The Conditions tab of the scheduled task's Properties dialog box



Settings Properties

The Settings tab (Figure 11.51) shows the settings that affect the task's behavior. You can specify the following settings:

- Whether the task can be run on demand
- Whether the task should be restarted if it is missed
- How often the task should be restarted if it fails
- When to stop the task if it runs a long time
- Whether you can force the task to stop
- When the task should be deleted
- What actions should occur if the task is already running

History Properties

The History tab (Figure 11.52) shows historical information regarding the task, including the task's start time, stop time, and whether the task completed successfully.

FIGURE 11.51 The Settings tab of the scheduled task's Properties dialog box

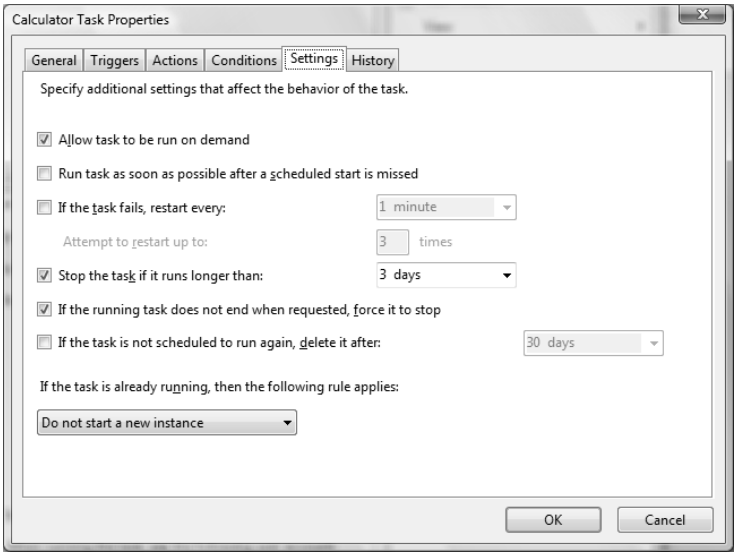
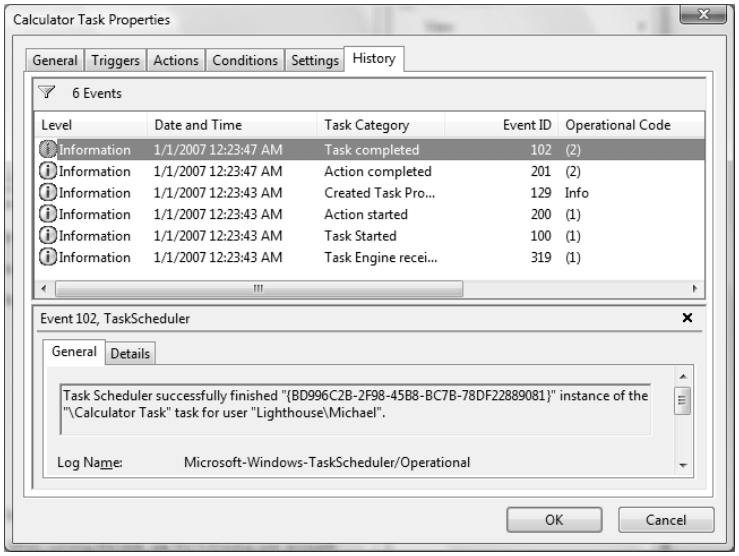


FIGURE 11.52 The History tab of the scheduled task's Properties dialog box



Troubleshooting Scheduled Tasks

If you are trying to use Task Scheduler and the tasks are not properly being executed, one of the following troubleshooting options may resolve the problem:

- If a scheduled task does not run as expected, right-click the task and select Properties. In the Task Scheduler Library, ensure that the task status is Ready. In the task's properties page, verify the schedule has been defined on the Triggers tab.
- If the scheduled task is a command-line utility, make sure that you have properly defined the command-line utility, including any options that are required for the utility to run properly.
- Verify that the user who is configured to run the scheduled task has the necessary permissions to the task that will be run.
- Within the Task Status section, check the task status to see when the task last ran successfully, if ever.
- Verify that the Task Scheduler service has been enabled on the computer if no tasks can be run on the computer.

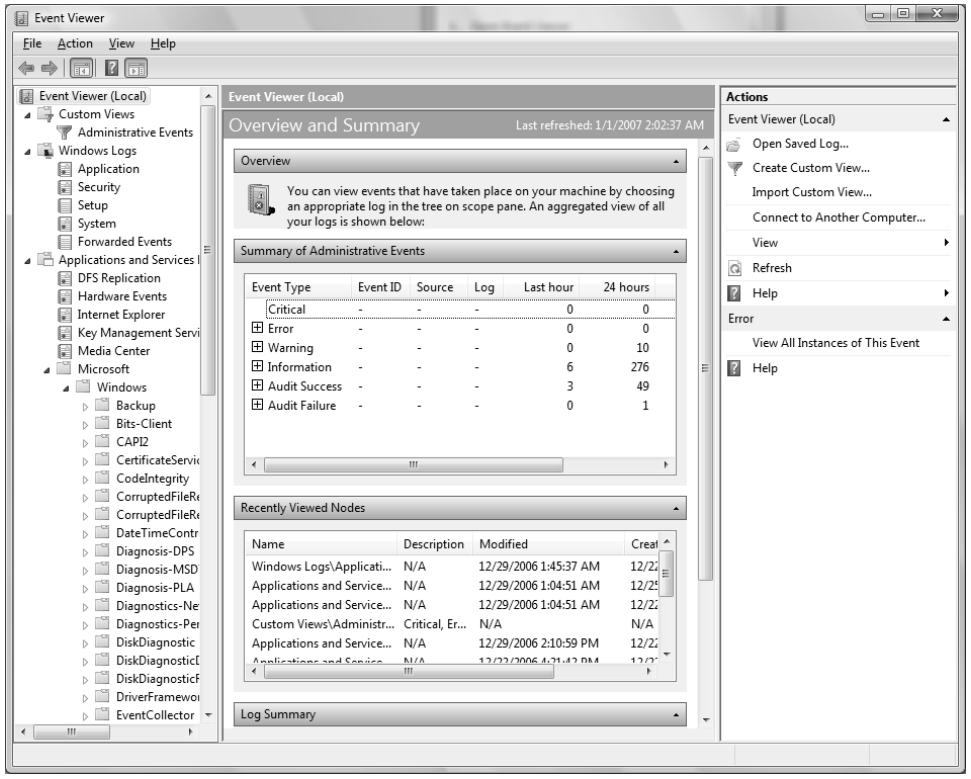
Using Event Viewer

Event Viewer has also been overhauled for Windows Vista. Event Viewer, shown in Figure 11.53, enables you to view event logs that are created by the operating system. This utility is very useful when troubleshooting problems that occur on your computer. Whenever an error occurs, an event is usually placed in one or more event logs. To open Event Viewer, click Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools ➢ Event Viewer. Alternatively, you can right-click Computer, choose Manage from the context menu, and open Event Viewer under System Tools.

Whereas old versions of Event Viewer contained only the Application, Security, and System logs, Windows Vista's version of Event Viewer contains the following Windows Logs:

- Application
- Security

FIGURE 11.53 Event Viewer



- Setup
- System
- Forwarded Events

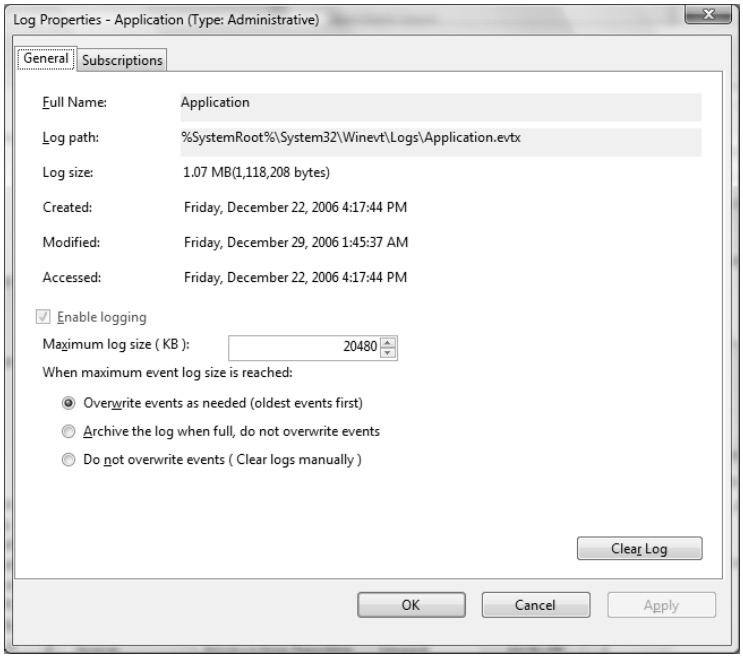
The Application log is used to log events relating to applications, such as whether an application, driver, or service fails. The Security log is used to log security events, such as successful or failed logon events. The Setup log is used only by domain controllers, so it doesn't have much practical use in Windows Vista. The System log is used to log events related to the operating system and related services. The Forwarded Events log is used to collect events that have been forwarded from other computers.

To configure log settings, right-click the log that you want to configure and select Properties. The Log Properties dialog box will appear, as shown in Figure 11.54.

The Log Properties dialog box will show the following information:

- Where the log is stored
- The size of the log
- When the log was created, modified, and accessed
- Whether logging is enabled for the log
- The maximum log size in KB
- The action that occurs when the log reaches the maximum size

FIGURE 11.54 Log Properties dialog box



When the log reaches the maximum size, you can configure Event Viewer to overwrite events, archive the log, or require that the event log be cleared manually.

If you notice that events are not being displayed, be sure that logging is enabled for the log, and that the log is not configured to overwrite events when it is full.

The left pane of Event Viewer also contains other logs and views that can be helpful when troubleshooting a specific application. The Custom Views section can be used to create a view that contains only the information you want to see, such as only events in a particular log, or only Critical events. One custom view, Administrative Events, is created for you by default. The Administrative Events view contains Critical, Error, and Warning events from all logs, enabling you to easily view only the most important events.

Another section contains logs relating to Applications and Services. This section contains six subsections:

- DFS Replication
- Hardware Events
- Internet Explorer
- Key Management Service
- Media Center
- Microsoft

The Microsoft folder contains many other logs related to specific Microsoft components and applications.

Finally, the Subscription folder enables you to receive event logs from other computers. To use subscriptions, the Windows Event Collector Service must be started.

The center pane of Event Viewer displays the events and information relating to those events. You can also view a summary of your administrative events, which contains a count of Critical, Error, Warning, Information, Audit Success, and Audit Failure events. A count of these events is displayed for the last hour, day, and week, and the total number of events is also provided.

Each event is assigned an event level. The following list displays the event levels from most severe to least severe:

- Critical
- Error
- Warning
- Information
- Verbose

The right pane of Event Viewer enables you to perform actions related to items you have selected in the left and center panes. You can save logs, open saved logs, create or import

views, clear logs, filter logs, and find logs with certain keywords. You can also attach a task to an event. Clicking Attach Task to This Event will open the Create Basic Task Wizard in Task Scheduler so that you can easily create a task related to the selected event.

We discussed Task Scheduler earlier in this chapter.

When you click on an event, information about the event is displayed at the bottom of the center pane. You can typically click a link at the bottom of the General tab in order to get more information online about the event. This information can often tell you how to fix the problem that is occurring.

In Exercise 11.10, you will view events in Event Viewer and set log properties.

EXERCISE 11.10

Using the Event Viewer Utility

1. Select Start ➢ Control Panel ➢ System and Maintenance ➢ Administrative Tools ➢ Event Viewer. Alternatively, you can right-click Computer, choose Manage from the context menu, and open Event Viewer under System Tools.
2. Open Windows Logs and click System in the left pane of the Event Viewer window to display the System log events.
3. Double-click the first event in the center pane of the Event Viewer window to see its Event Properties dialog box. Click the Close button to close the dialog box.
4. Right-click System in the left pane of the Event Viewer window and select Properties.
5. Configure the System log to archive the log file when it is full by clicking Archive The Log File When Full; Do Not Overwrite Events. Click OK to close the dialog box.
6. Right-click System in the left pane of the Event Viewer window and select Filter Current Log.
7. Select the check boxes next to Critical and Error boxes; then click OK. You should see only Critical and Error events listed in the System log.
8. Right-click System and select Clear Log.
9. A dialog box will appear asking if you want to save the System log before clearing it. Click the Save and Clear button.
10. Specify the path and filename for the log file, and then click the Save button. The events will be saved in an `.evtx` file, and the events will be cleared from the System log.

Real World Scenario

Using Event Viewer Logs for Problem Resolution

You are a senior network engineer for a company using specialized hardware and software that is run on Windows Vista computers in the field. One of your junior network engineers is on site in another state. She is reporting errors with your software and hardware but is not able to diagnose the problem.

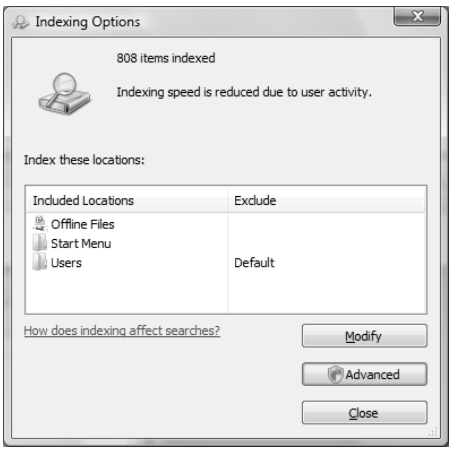
You want to be able to troubleshoot the problem remotely if possible. One way that you can view a complete history of any informational, warning, or error messages is to have the on-site engineer send the log files to you or to another senior engineer. To do this, the on-site engineer right-clicks on a log, selects Save Events As, and saves the log file to a file that will automatically be given an `.evtx` extension. These EVTX files can then be e-mailed to the more experienced engineer for problem resolution. Another way you can view log files remotely is to configure a subscription. Finally, you can use Remote Desktop to remotely administer the computer.

The Event Viewer is a handy utility because it lets you track information about your computer's hardware and software. You can also use it to monitor security events.

Using Indexing Options

Indexing Options enables your computer to quickly find files when you search for them. To access Indexing Options, click Start ➢ Control Panel ➢ System and Maintenance ➢ Indexing Tools. The Indexing Tools dialog box will appear, as shown in Figure 11.55.

FIGURE 11.55 Indexing Options



By default, files that you would be likely to search for are indexed, such as the Users folder and subfolders. Since users don't usually search for program files and system files, folders that contain these items are not indexed by default. However, you can add or remove locations to be indexed by clicking the Modify button.

Although you can index every file in every location on your computer, you shouldn't. Doing so will increase the size of your index and reduce the performance of your searches.

The Advanced button brings up the Advanced Options dialog box. The Advanced Options dialog box contains two tabs: Index Settings and File Types. The Index Settings tab is shown in Figure 11.56. Under File Settings, you can select whether encrypted files are indexed, and whether words with diacritics (such as accent marks) are searched when the specific diacritic character isn't used. Under Troubleshooting, you can choose to rebuild the index and to restore the index to its default configuration. Under Index Location, you can select where your index is stored, and you can move the index to a new location.

The File Types tab is shown in Figure 11.57. This tab is used to select which files are indexed and how they are indexed. You can select to index only the file's properties, or you can select to index both the file's properties and its contents. If a particular file extension is not listed, you can add it by typing it in the field at the bottom of the dialog box and clicking Add New Extension.

FIGURE 11.56 Advanced Options, Index Settings tab

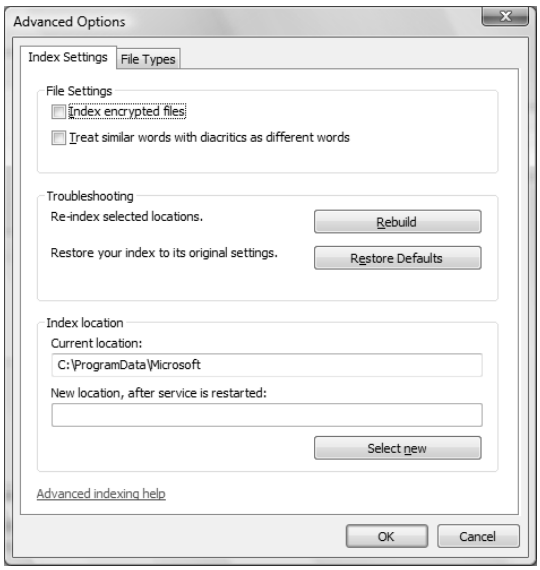
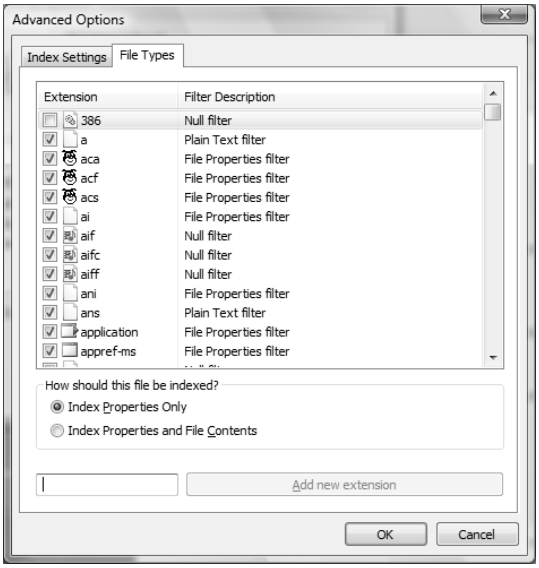


FIGURE 11.57 Advanced Options, File Types tab



Using Remote Desktop and Remote Assistance

Remote Desktop is a service that allows you to remotely take control of your computer from another location. For example, you could access your work computer from home or while traveling on business. *Remote Assistance* is used to request assistance from another user.

You will learn more about Remote Desktop and Remote Assistance in the following sections.

Using Remote Desktop

Remote Desktop is a tool in Windows Vista that allows you to take control of a remote computer's keyboard, video, and mouse. This tool does not require that someone collaborate with you on the remote computer. While the remote computer is being accessed, it remains locked and any actions that are performed remotely will not be visible to the monitor that is attached to the remote computer. Remote Desktop is designed to be used in the following situations:

- For troubleshooting computers within an organization that may be in a remote location but are connected to the central network through a direct network connection, secure virtual private network (VPN), or remote access

- To allow help desk administrators within a network to remotely troubleshoot organizational computers
- To allow remote access to organizational computers without security concerns that unauthorized users are viewing the remote computer's monitor and watching what actions are being performed remotely

In the following sections you will learn

- The Remote Desktop restrictions
- The minimum set of requirements for Remote Desktop
- How to configure the computer that will be accessed remotely
- How to configure the computer that will be used to access the remote computer
- How to start a Remote Desktop session
- How to customize a Remote Desktop session
- How to end a Remote Desktop session

Remote Desktop Restrictions

Remote Desktop uses all of the inherent security features of Windows Vista. In addition, Remote Desktop imposes these additional security features:

- If you want to establish a session from a computer via the Internet to your company's internal network, you must first establish a secure VPN connection to the internal network you wish to access.
- Remote Desktop can't be used to create a connection between two computers directly connected to the Internet. However, you can use Remote Desktop Web Connection.
- There is no option for simultaneous remote and local access to the Windows Vista Desktop. If someone logs into a computer remotely using Remote Desktop, Windows Vista will log the local user off; if the local user logs back on, the remote user will be logged off.

Remote Desktop Requirements

To use Remote Desktop, the following requirements must be met:

- Windows XP Professional or Windows Vista must be running on the computer that will be accessed remotely.
- The computer that will access the remote computer must be running Windows 95 or higher and have Remote Desktop client software installed and configured.
- There must be an IP connection between the two computers that will be used to establish a Remote Desktop session.

Configuring a Computer for Remote Desktop

To enable a remote computer to allow Remote Desktop access, select Start ➢ Control Panel ➢ System and Maintenance ➢ System. Click Remote Settings in the left pane. Within the Remote

tab of System Properties, check either Allow Connections from Computers Running Any Version of Remote Desktop (less secure) or Allow Connections Only from Computers Running Remote Desktop with Network Level Authentication (more secure), as shown in Figure 11.58. Network Level Authentication (NLA) is used natively by Windows Vista and Windows Server 2007 with Remote Desktop.

The Remote Desktop 6.0 client update can be installed on computers running Windows XP with SP2 and Windows Server 2003 with SP1 that will allow these computers to use NLA. You can download the Remote Desktop 6.0 client update from `http://support.microsoft.com/kb/925876`.

To enable remote access, you must be logged on to the computer as an administrator or a member of the Administrators group.

By default, only members of the Administrators group can access a computer that has been configured to use Remote Desktop. To enable other users to access the computer remotely, click the Select Users button shown in Figure 11.58. This brings up the Remote Desktop Users dialog box, as shown in Figure 11.59, and allows you to specify which users can access the remote computer by selecting users through the Add or Remove buttons.

FIGURE 11.58 The Remote tab of the System Properties dialog box

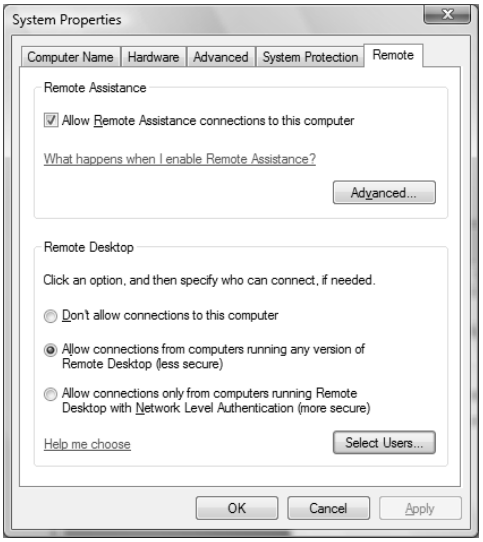
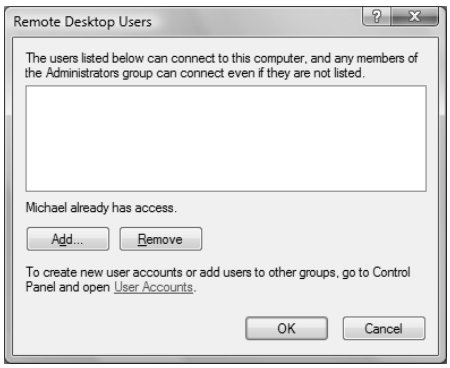


FIGURE 11.59 The Remote Desktop Users dialog box



When you enable remote access to a computer, the changes will take effect immediately. By default, members of the local Administrators or Domain Administrators group will have Remote Desktop permissions. Members of the Administrators group can end a local user's session without permission of the user. Nonadministrative users who are granted Remote Desktop permissions can't end a local user's session if the local user refuses the session.

In addition to enabling Remote Desktop, you may also need to configure an exception in Windows Firewall, if Windows Firewall is enabled. To do this, perform the following steps:

1. Open Windows Firewall by clicking Start ➢ Control Panel ➢ Security Center ➢ Windows Firewall.
2. Select Allow a Program Through Windows Firewall in the left pane.
3. On the Exceptions tab, ensure the Remote Desktop check box is selected. Click OK or Apply to apply the settings.

If you are unable to connect to a computer using Remote Desktop, you should ensure that Block All Incoming Connections is not selected on Windows Firewall. When Block All Incoming Connections is selected, exceptions are ignored.

Installing the Remote Desktop Client Software

The Remote Desktop Connection client software is used to control a Windows-based computer remotely. This software is installed by default on computers running Windows Vista Business, Windows Vista Enterprise, Windows Vista Ultimate, Windows XP Home, and Windows XP

Professional. The Remote Desktop Communications client software is used for Remote Desktop support on pre–Windows XP clients, which are listed in this section.

You can also install the Remote Desktop Communications client software on the following computers:

- Windows 95
- Windows 98
- Windows Me
- Windows NT 4
- Windows 2000

Starting a Remote Desktop Session

Once you have configured the computer that will be accessed remotely and have installed the Remote Desktop Connection client software, you are ready to start a Remote Desktop session. You start a session using these steps:

1. Start ➢ All Programs ➢ Accessories ➢ Remote Desktop Connection. You can also use the command-line utility MSTSC to start the Remote Desktop connection. This will bring up the dialog box shown in Figure 11.60.
2. In the Computer name field, type in the name or IP address of the computer you wish to access. Remote Desktop must be enabled on this computer and you must have permissions to access the computer remotely.
3. Click the Connect button.
4. The Windows Security dialog box will appear. Type in your username, password, and domain name, and click OK.

If the remote computer is running an operating system older than Windows Vista, or configured to support only the RDP security layer, then the identity of the computer cannot be verified. You will be asked whether you want to connect anyway. Click Yes to proceed.

5. The Remote Desktop Connection window will open, and you will now have remote access.

FIGURE 11.60 The Remote Desktop Connection dialog box

Once a workstation-based computer has been accessed remotely, it will be locked at the console. No one at the local site will be able to use the local computer without a password. In addition, no one at the local site will be able to see the work that is being done on the computer remotely.

When using Remote Desktop, only one person at a time can control a workstation-based computer. However, several people can simultaneously connect to and use a server-based computer using Remote Desktop.

Customizing a Remote Desktop Connection

You can manage your Remote Desktop connection settings by clicking the Options button that was shown in Figure 11.60. This brings up the dialog box shown in Figure 11.61. In this dialog box you can configure the following:

General Contains logon settings. You can also save the current connection settings to an RDP file. By default, settings are saved in the `My Documents\Remote Desktop` folder.

Display Used to set the size of the remote desktop, the colors used by the remote desktop, and whether the connection bar will be displayed in full-screen mode.

Local Resources Used to specify whether you hear remote computer sounds, the Windows keyboard combinations that will be applied, and which local devices you will automatically connect to on the local computer. These local devices include printers, floppy drives, hard drives, optical drives, flash media, serial ports, and smart cards.

If you want to be able to copy information between the host computer and the remote computer without creating a network share, you must select the host computer's drives by clicking the More button on the Local Resources tab before connecting to the remote computer.

Programs Allows you to start a program on connection.

Experience Used to optimize performance based on your connection speed. The faster your connection is, the more features you will be able to see. You can also select whether the connection will be reestablished if it is dropped.

If you are not able to see certain visual features on the remote computer, check the Experience tab to ensure that they are selected. For example, if you want to be able to see the desktop background and use font smoothing on the remote computer, you must select LAN (10Mbps or higher) or Custom. The Broadband and Modem selections do not allow these options.

Advanced Used to configure options for server authentication options and settings for Terminal Services Gateway, which can be used to connect to a remote computer behind a firewall.

FIGURE 11.61 The Remote Desktop Connection options

Ending a Remote Desktop Session

If disconnecting from a Windows Vista computer, select Start ➢ X on the remote computer; the X button disconnects your session. When disconnecting from older operating systems, select Start ➢ Disconnect. Windows will confirm whether you want to disconnect. Click Disconnect to confirm.

Connecting by Using Remote Desktop Web Connection

Remote Desktop Web Connection enables you to connect to a remote computer over the Internet. Before you can connect, Remote Desktop Web Connection must be installed on the remote computer.

To connect to a remote computer, follow these steps:

1. Open Internet Explorer or another web browser and type the name or IP address of the remote computer, followed by **`/tsweb/`**. For example, to connect to a computer named brainbeacon, type **`http://brainbeacon/tsweb/`**.
2. On the logon screen, type the remote computer name, specify the screen size, and click Connect.
3. Type your username and password and click OK.
4. To disconnect, log off and close your web browser.

If you are having trouble connecting using Remote Desktop Web Connection, ensure that your firewall allows TCP port 80.

Using Remote Assistance

Remote Assistance provides a mechanism for requesting help by instant message or e-mail. To use Remote Assistance, the computer requesting help and the computer providing help must be using Windows Vista, Windows XP Professional, or Windows Server 2003, and both computers must have interconnectivity.

When assisting a user, you can use text-based chat or send files back and forth. You can also take control of a user's desktop. Common examples of when you would use Remote Assistance include the following:

- Use Remote Assistance when you are diagnosing problems that are difficult to explain or reproduce. By using Remote Assistance, you can remotely view the computer and the remote user can show you what the error is or step you through the processes that cause the error to occur.
- Use Remote Assistance when you need an inexperienced user to perform a complex set of instructions. Instead of asking the inexperienced user to complete the task, you can use Remote Assistance to take control of the computer and complete the tasks yourself.

In the following sections you will learn more about

- Differences between Remote Desktop and Remote Assistance
- Options for establishing remote connections
- Enabling Remote Assistance
- How users request remote assistance
- How administrators respond to remote assistance requests
- Administrator-initiated remote assistance
- Limitations of Remote Assistance invitations
- Security and Remote Assistance

Voice-based chat, which was available in Remote Assistance on Windows XP and Windows Server 2003, is no longer available in Windows Vista.

Differences between Remote Desktop and Remote Assistance

The key differences between the Remote Desktop utility and the Remote Assistance utility are as follows:

- With Remote Desktop, there is only one user connected at a time. With Remote Assistance, a user is able to establish a concurrent session with the user at the remote computer so both users can see the same desktop.

- Remote Assistance requires the user at the remote computer to authorize access. Remote Desktop does not require an administrator or authorized user to seek permission before establishing a remote session.
- With Remote Assistance, both computers have to be running Windows XP Professional, Windows Server 2003, or Windows Vista.

Options for Establishing Remote Assistance

The following options can be used to establish remote connections:

- A local area network connection between the expert's computer and the novice's computer
- An Internet connection between the expert's computer and the novice's computer
- Connection via the Internet when the expert computer is behind a firewall and the novice computer is just connected to the Internet
- Connection via the Internet when the expert computer is behind a firewall and the novice computer is also behind a firewall

If the Remote Assistance connections are made through a firewall, the firewall may need to be configured to open TCP port 3389.

Enabling Remote Assistance

You can enable Remote Assistance on a remote computer through the following steps:

1. Select Start ➢ Control Panel ➢ Performance and Maintenance ➢ System.
2. Click Remote Settings in the left pane.
3. On the Remote tab of System Properties, select Allow Remote Assistance Connections to This Computer, as shown in Figure 11.62.

If you click the Advanced button on the Remote tab, you can set the following configuration options in the Remote Assistance Settings dialog box, shown in Figure 11.63:

- Whether you allow the computer to be controlled remotely
- The maximum amount of time that invitations will remain open, specified in minutes, hours, or days
- Whether invitations are accepted only from computers running Windows Vista or later

By default, invitations remain open for six hours.

FIGURE 11.62 The Remote tab of the System Properties dialog box

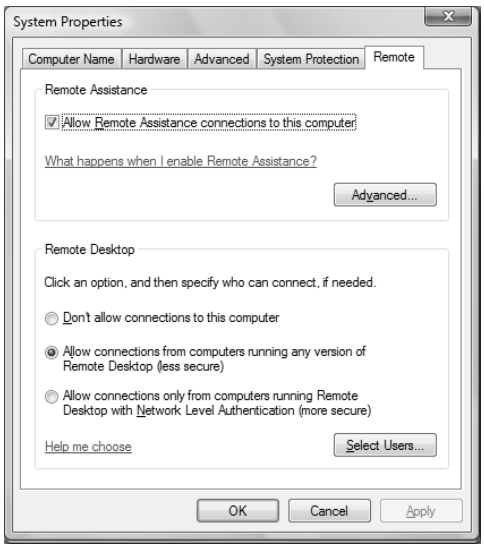
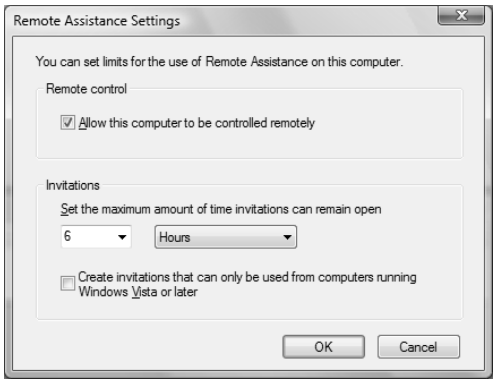


FIGURE 11.63 The Remote Assistance Settings dialog box



In addition to enabling Remote Assistance, you may also need to configure an exception in Windows Firewall, if Windows Firewall is enabled. To do this, perform the following steps:

1. Open Windows Firewall by clicking Start ➢ Control Panel ➢ Security Center ➢ Windows Firewall.
2. Select Allow a Program Through Windows Firewall in the left pane.
3. On the Exceptions tab, ensure the Remote Assistance check box is selected. Click OK or Apply to apply the settings.

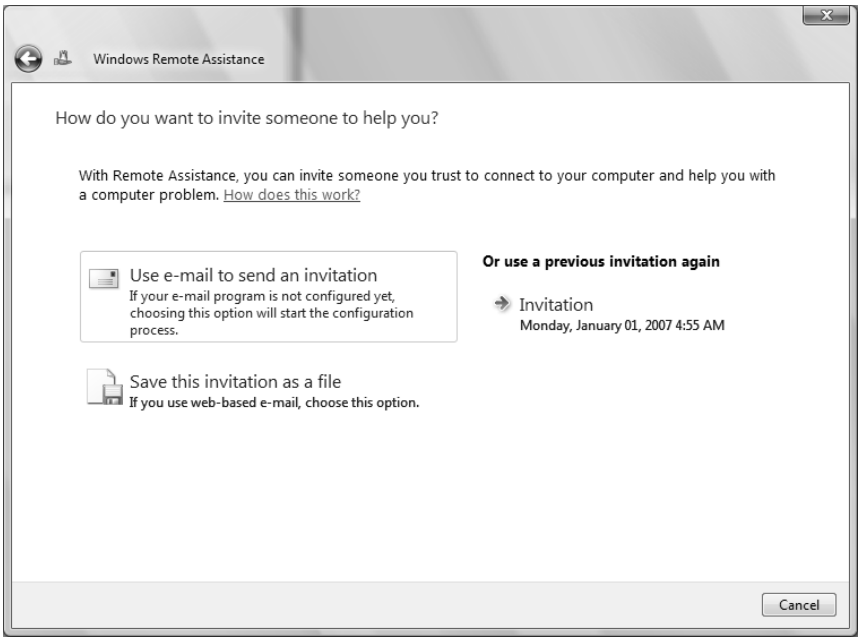
If you are unable to connect to a computer using Remote Assistance, you should ensure that Block All Incoming Connections is not selected on Windows Firewall. When Block All Incoming Connections is selected, exceptions are ignored.

Requesting Remote Assistance

If a user requires remote assistance, they can send an invitation. The following steps are used to request remote assistance:

1. Notify the person providing assistance that you will be sending a Remote Assistance invitation. Notification methods might include e-mail, instant messaging, or a telephone call. Give the person providing assistance the password that will be used for the Remote Assistance session.
2. Select Start ➢ All Programs ➢ Maintenance ➢ Windows Remote Assistance. The Windows Remote Assistance dialog box will appear, as shown in Figure 11.64.
3. Select Invite Someone You Trust To Help You.
4. Select either Use E-mail to Send An Invitation or Save This Invitation as a File. If an invitation has previously been sent, you can use it again.

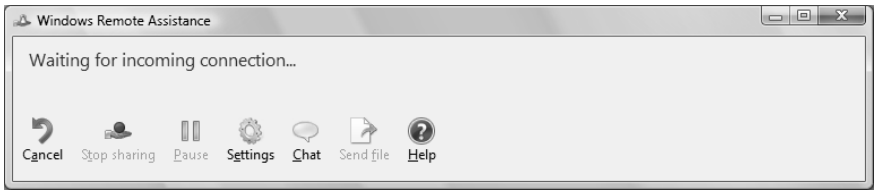
FIGURE 11.64 Windows Remote Assistance



5. To send the invitation by e-mail, type the password, confirm the password, and click Next. Your e-mail program will open up with the Remote Assistance invitation attached and a preconfigured message already typed. Type the recipient's e-mail address and click Send.
6. To save the invitation as a file, enter a path and filename, type a password, and confirm the password. Click Finish to save the file.
7. The Windows Remote Assistance window will appear, as shown in Figure 11.65, and will wait for an incoming connection.

By default, the invitation will be saved with an `.msrcincident` extension.

FIGURE 11.65 Windows Remote Assistance, waiting for an incoming connection



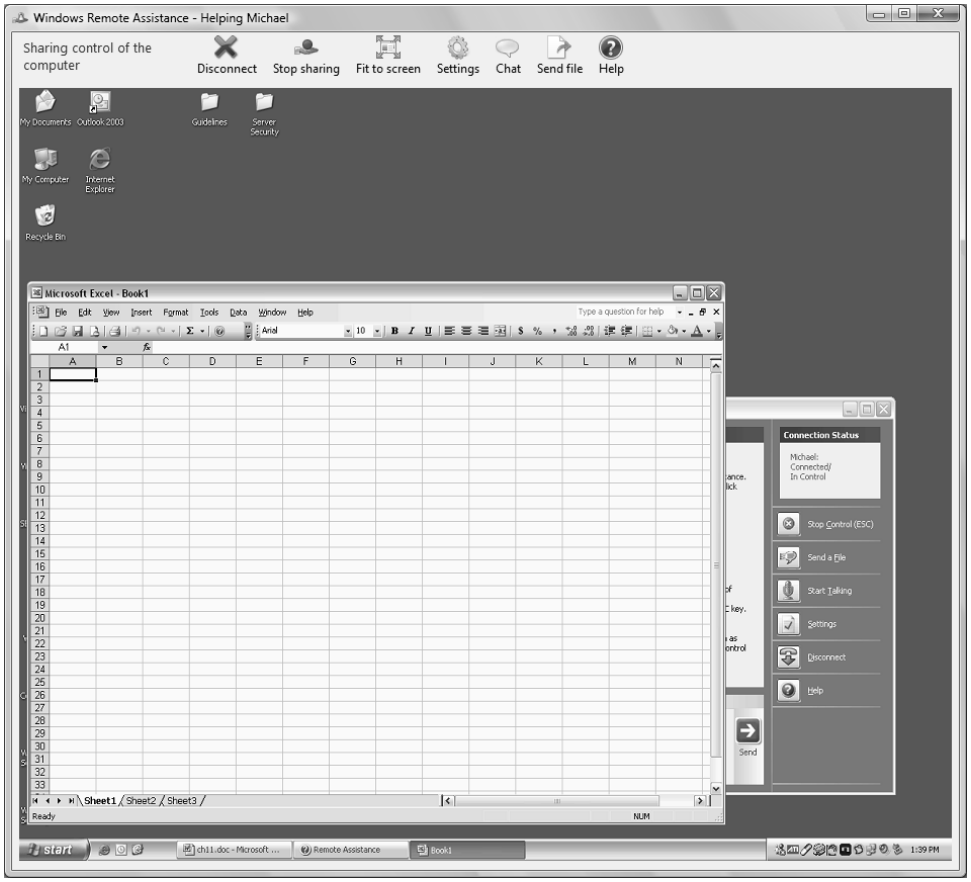
Responding to Remote Assistance Requests

When you receive a Remote Assistance invitation, you would use the following steps to respond:

1. Receive the Remote Assistance invitation.
2. Open the invitation file, provide the appropriate password, and click Yes to continue.
3. The user seeking assistance will see an acceptance message on their screen and be prompted to verify that you be allowed to view the remote screen.
4. After the user confirms the acceptance message, a terminal window will display the user's desktop, as shown in Figure 11.66.
5. You will then be able to manipulate remotely the user's computer by using the Request Control option. The user must then allow you to share control of their desktop.

The assisted user can stop sharing control of the desktop by clicking the Stop Sharing button (or the Stop Control button on Windows XP). Either user can terminate the session at any time by clicking the Disconnect button in the Remote Assistance window.

FIGURE 11.66 Remote Assistance session



By default, a Remote Assistance invitation automatically expires after six hours. The expiration time period for created invitations can be changed by clicking the Advanced button on the Remote tab of the System Properties dialog box.

If a Windows Vista user wants to expire an invitation early, they can do so by closing the Windows Remote Assistance session.

Initiating a Remote Assistance Session

Administrators can also initiate a remote assistance session. Once Remote Assistance is enabled, you can offer remote assistance to a user through the following steps:

1. Inform the user that you will be offering remote assistance.
2. Select Start ➢ All Programs ➢ Maintenance ➢ Windows Remote Assistance.
3. Select Offer to Help Someone.

4. Enter the location of an invitation file, select a previously used invitation, or type a computer name or IP address.
5. The user will see a prompt that you would like to view the screen. The user then accepts your assistance request.

You cannot offer assistance to a Windows XP or Windows Server 2003 computer without an invitation.

Security and Remote Assistance

Security and security configuration concerns when using Remote Assistance include the following:

- If a user allows a user to take control of the desktop, then the person providing expert assistance will have all of the security privileges that the local user has.
- If you allow a user outside of your organization to access your computer, you should have them connect via a VPN account. If they connect through the network firewall, then TCP port 3389 must be opened.

Safeguarding Your Computer and Recovering from Disaster

One of the worst events you will experience is a computer that won't boot. An even worse experience is discovering that there is no recent backup for that computer.

The first step in preparing for disaster recovery is to expect that a disaster will happen at some point and take proactive measures to plan your recovery before the failure occurs. Here are some of the preparations you can make:

- Keep your computer up-to-date with Windows Update (covered in Chapter 1).
- Perform regular system backups.
- Use current software to scan for malware (such as viruses, spyware, and adware) and make sure you have the most recent updates.
- Perform regular administrative functions, such as monitoring the logs in the Event Viewer utility.

If you can't start Windows Vista, there are several options and utilities that can be used to identify and resolve Windows errors. The following is a broad list of troubleshooting options:

- If you have recently made a change to your computer's configuration by installing a new device driver or application and Windows Vista will not load properly, you can use the Last Known Good Configuration, roll back the driver, or use System Restore to restore a previous system configuration.

- If you can boot your computer to Safe Mode, and you suspect that you have a system conflict, you can temporarily disable an application or processes, troubleshoot services, or uninstall software.
- If your computer will not boot to Safe Mode, you can use the Startup Repair Tool to replace corrupted system files.
- If necessary, you can use the Backup and Restore Center utility to restore personal files from backup media and to restore a complete image of your computer.

Table 11.3 summarizes all of the Windows Vista utilities and options that can be used to assist in performing system recovery.

All these Windows Vista recovery techniques are covered in detail in this chapter.

TABLE 11.3 Windows Vista Recovery Techniques

Recovery Technique	When to Use
Event Viewer	If the Windows Vista operating system can be loaded through Normal or Safe Mode, one of the first places to look for hints about the problem is Event Viewer. Event Viewer displays System, Security, and Application logs.
Safe Mode	This is generally your starting point for system recovery. Safe Mode loads the absolute minimum of services and drivers that are needed to boot Windows Vista. If you can load Safe Mode, you may be able to troubleshoot devices or services that keep Windows Vista from loading normally.
Last Known Good Configuration	This option can help if you made changes to your computer and are now having problems. Last Known Good Configuration is an Advanced Boot Options menu item that you can select during startup. It loads the configuration that was used the last time the computer booted successfully. This option will not help if you have hardware errors.
Startup Repair Tool	This tool can restore system files from the Windows Vista media. This option will not help if you have hardware errors.
Backup and Restore Center	You should use this utility to safeguard your computer. Through the Backup utility, you can back up and restore personal files on your computer. You can also create and restore images of your entire computer.
System Restore	System Restore is used to create known checkpoints of your system's configuration. In the event that your system becomes misconfigured, you can restore the system configuration to an earlier checkpoint.

Using Advanced Boot Options

The Windows Vista advanced startup options can be used to troubleshoot errors that keep Windows Vista from successfully booting.

To access the Windows Vista advanced startup options, start or reboot the computer and press the F8 key after the firmware POST process, but before Windows Vista is loaded. This will bring up the Advanced Boot Options menu, which offers numerous options for booting Windows Vista.

These advanced startup options are covered in the following three sections.

Starting in Safe Mode

When your computer will not start, one of the fundamental troubleshooting techniques is to simplify the configuration as much as possible. This is especially important when you do not know the cause of your problem and you have a complex configuration. After you have simplified the configuration, you can determine whether the problem is in the basic configuration or is a result of your complex configuration. If the problem is in the basic configuration, you have a starting point for troubleshooting. If the problem is not in the basic configuration, you should proceed to restore each configuration option you removed, one at a time. This helps you to identify what is causing the error.

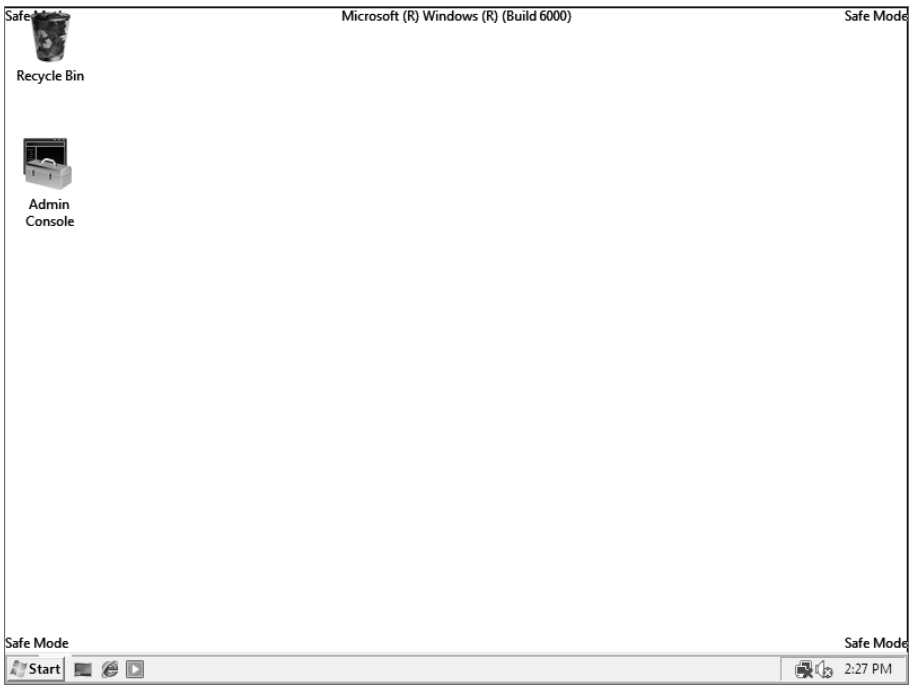
If Windows Vista will not load, you can attempt to load the operating system through *Safe Mode*. When you run Windows Vista in Safe Mode, you are simplifying your Windows configuration as much as possible. Safe Mode loads only the drivers needed to get the computer up and running. The drivers that are loaded with Safe Mode include basic files and drivers for the mouse, monitor, keyboard, hard drive, standard video driver, and default system services. Safe Mode is considered a diagnostic mode, so you do not have access to all of the features and devices in Windows Vista that you have access to when you boot normally, including networking capabilities.

A computer booted to Safe Mode will show "Safe Mode" in the four corners of your Desktop, as shown in Figure 11.67.

If you boot to Safe Mode, check all of your computer's hardware and software settings in Device Manager (which is covered in Chapter 3) and try to determine why Windows Vista will not boot properly. After you take steps to fix the problem, try to boot to Windows Vista as you normally would.

In Exercise 11.11, you will boot your computer to Safe Mode.

FIGURE 11.67 A computer running in Safe Mode



EXERCISE 11.11

Booting Your Computer to Safe Mode

1. If your computer is currently running, select Start ➢ Shutdown ➢ Restart.
2. During the boot process, press the F8 key to access the Advanced Boot Options menu.
3. Highlight Safe Mode and press Enter.
4. When Windows Vista starts, log in.
5. You will see a Help and Support dialog box letting you know what Safe Mode is. Exit Help and Support.
6. You should see in the lower-right corner that a network connection is not available.

EXERCISE 11.11 *(continued)*

7. Select Start ➢ Control Panel. Notice that most of the Control Panel icons are not available. If you are having a problem with a driver, you can open Device Manager and uninstall or roll back the driver.

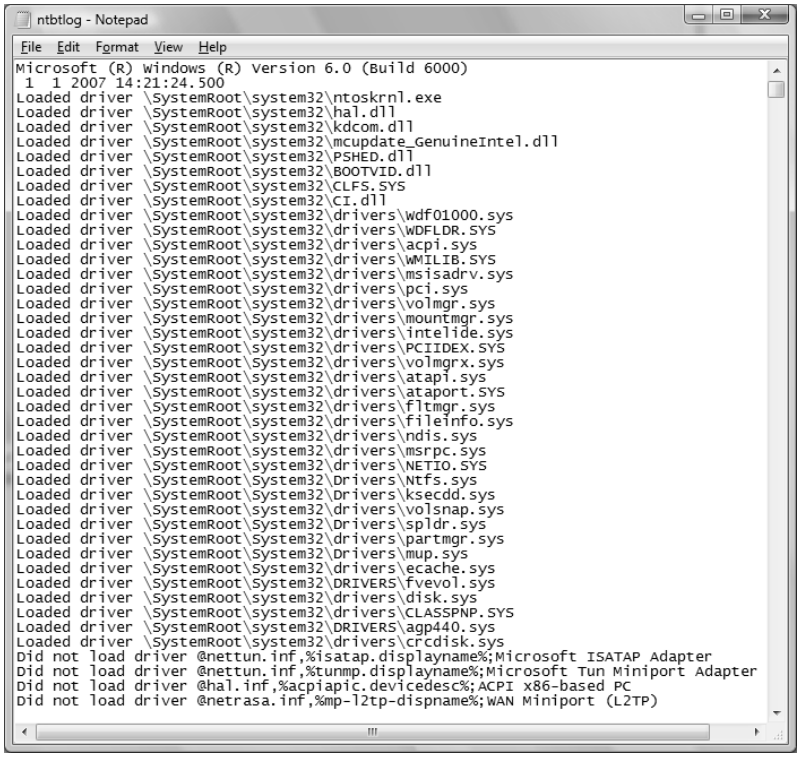
8. Don't restart your computer yet; you will do this as a part of the next exercise.

Enabling Boot Logging

Boot logging creates a log file that tracks the loading of drivers and services. When you choose the *Enable Boot Logging* option from the Advanced Boot Options menu, Windows Vista loads normally, not in Safe Mode. This allows you to log all of the processes that take place during a normal boot sequence.

This log file can be used to troubleshoot the boot process. When logging is enabled, the log file is written to `\Windows\Ntbtlog.txt`. A sample of the `Ntbtlog.txt` file is shown in Figure 11.68.

FIGURE 11.68 The Windows Vista boot log file



In Exercise 11.12, you will create and access a boot log file.

EXERCISE 11.12

Using Boot Logging

1. Start your computer. If it is already running, select Start ➢ Restart.
2. During the boot process, press the F8 key to access the Advanced Boot Options menu.
3. Highlight Enable Boot Logging and press Enter.
4. When Windows Vista starts, log in.
5. Select Start ➢ Computer and browse to `C:\WINDOWS\Ntbtlog.txt`. Double-click this file.
6. Examine the contents of your boot log file.
7. Shut down your computer and restart it without using Advanced Boot Options.

The boot log file is cumulative. Each time you boot to Safe Mode, you are writing to this file. This allows you to make changes, reboot, and see if you have fixed any problems. If you want to start from scratch, you should manually delete this file and reboot to an Advanced Boot Options menu selection that supports logging.

Using Other Advanced Boot Options Menu Modes

In this section, you will learn about additional Advanced Boot Options menu modes. These include the following:

Safe Mode with Networking This is the same as the Safe Mode option but adds networking features. You might use this mode if you need networking capabilities to download drivers or service packs from a network location.

Safe Mode with Command Prompt This starts the computer in Safe Mode, but after you log in to Windows Vista, only a command prompt is displayed. This mode does not provide access to the desktop. Experienced troubleshooters use this mode.

Enable Low-Resolution Video (640x480) This loads a standard VGA driver without starting the computer in Safe Mode. You might use this mode if you changed your video driver, did not test it, and tried to boot to Windows Vista with a bad driver that would not allow you to access video. The Enable VGA Mode bails you out by loading a default driver, providing access to video so that you can properly install (and test!) the correct driver for your computer.

Safe Mode starts Windows Vista at a resolution of 800 × 600.

Last Known Good Configuration (advanced) This boots Windows Vista using the Registry information that was saved the last time the computer was successfully booted. You would use this option to restore configuration information if you have improperly configured the computer and have not successfully rebooted the computer. When you use the Last Known Good Configuration option, you lose any system configuration changes that were made since the computer last successfully booted.

Directory Services Restore Mode This option is used for domain controllers only and is not relevant to Windows Vista.

Debugging Mode This runs the Kernel Debugger, if it is installed. The Kernel Debugger is an advanced troubleshooting utility.

Disable Automatic Restart on System Failure Prevents Windows from restarting when a critical error causes Windows to fail. This option should be used only when Windows fails every time you restart so that you are not able to access the desktop or any configuration options.

Disable Driver Signature Enforcement Allows drivers to be installed even if they do not contain valid signatures.

Start Windows Normally This boots to Windows Vista in the default manner. This option is on the Advanced Boot Options menu in case you accidentally hit F8 during the boot process but really wanted to boot Windows Vista normally.

Using the Startup Repair Tool

If your Windows Vista computer will not boot because of missing or corrupted system files, you can use the *Startup Repair Tool* to correct these problems. Startup Repair cannot repair hardware failures. Additionally, Startup Repair cannot recover personal files that have been corrupted, damaged by viruses, or deleted. To ensure that you can recover your personal files, you should use the Backup and Restore Center utility.

To use the Startup Repair Tool, follow these steps:

1. Boot your computer using the Windows Vista media.
2. When the Install Windows dialog box appears, select the language, time and currency format, and the keyboard or input method. Click Next to continue.
3. The Install Now button will appear in the center of the screen. Click Repair Your Computer in the lower-left corner.
4. Select the operating system to recover and click Next. If you do not see your operating system, you might need to load your hard disk drivers by clicking the Load Drivers button.

5. The System Recovery Options dialog box will appear. You can choose one of the following options:
   - Startup Repair
   - System Restore
   - Windows Complete PC Restore
   - Windows Memory Diagnostic Tool
   - Command Prompt

   Choose Startup Repair to continue.
6. Startup Repair will check your computer for problems and attempt to repair them. After Startup Repair has finished, click Shut Down or Restart.

If you were not provided the Windows Vista media when you purchased your computer, the computer manufacturer might have placed the files on a recovery partition, or they might have replaced the Startup Repair Tool with one of their own. Check with the manufacturer for more information.

If Startup Repair is unable to correct the problem, you might have to reinstall Windows Vista. This should be done as a last resort.

Using Backup and Restore Center

The *Backup and Restore Center* utility allows you to create and restore backups. Backups protect your data in the event of system failure by storing the data on another medium, such a hard disk, CD, DVD, or network location. If your original data is lost due to corruption, deletion, or media failure, you can restore the data using your backup.

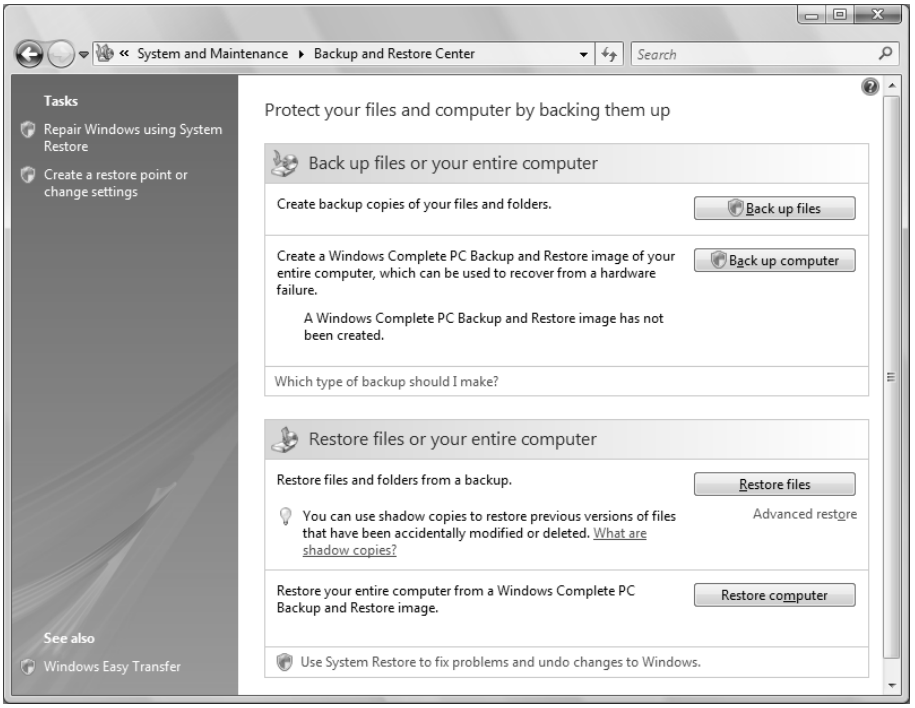
To access the Backup and Restore Center, select Start ➢ Control Panel ➢ System and Maintenance ➢ Backup and Restore Center. Alternatively, you can select Start ➢ All Programs ➢ Maintenance ➢ Backup and Restore Center. The Backup and Restore center is shown in Figure 11.69.

You can perform the following tasks with Backup and Restore Center:

- Back up files
- Restore files
- Change automatic backup settings
- Create an image of your entire computer
- Restore an image of your computer
- Restore a previous version of files or your computer using System Restore
- Create a restore point using System Protection

We will discuss each of these options in the following sections.

FIGURE 11.69 Backup and Restore Center



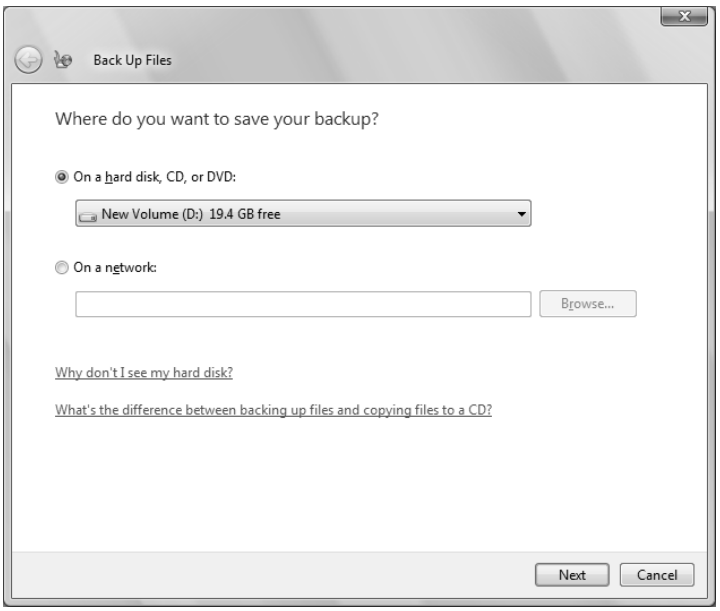
Backing Up Files

To create backup copies of your files and folders, click Back Up Files. The first time you create a backup, the Back Up Files dialog box will appear, as shown in Figure 11.70. After your first backup, the Back Up Files button will automatically back up your files based on the last backup you performed.

You can use Backup and Restore Center to back up the following types of files:

- Pictures
- Music
- Videos
- E-mail, including contact lists, `.pst` files, and `.eml` files
- Documents
- TV shows recorded from Windows Media Center
- Compressed files, such as those with `.zip`, `.cab`, `.iso`, `.wim`, and `.vhd` file extensions
- Additional files, which are files that do not correspond to any of the other categories.

FIGURE 11.70 Back Up Files



Backup and Restore Center will never back up the following files:

- System files
- Program files
- User Profile Settings
- Files encrypted by Encrypting File System (EFS)
- Files on FAT partitions
- Files in the Recycle Bin
- Temporary Files
- Web-based e-mail

To back up all the files and folders on your computer, you can use Windows Complete PC Backup to create an image of your entire computer.

You can also configure Backup and Restore Center to create a backup automatically. You can specify that backups occur daily, weekly, or monthly.

You cannot back up files to the same hard disk, the system disk (typically the C: drive), the boot disk (used to start your computer), or a USB flash drive.

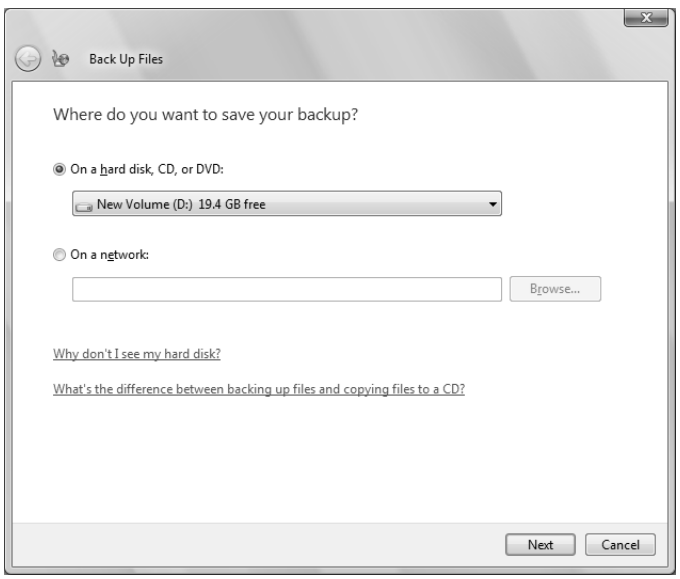
If a backup location is not available, be sure that it is formatted as an NTFS, FAT, or Universal Disk Format (UDF) partition.

In Exercise 11.13, you will make a backup of your files. This exercise assumes that you created a new volume in Exercise 7.2, and that you haven't yet configured an automatic backup.

EXERCISE 11.13

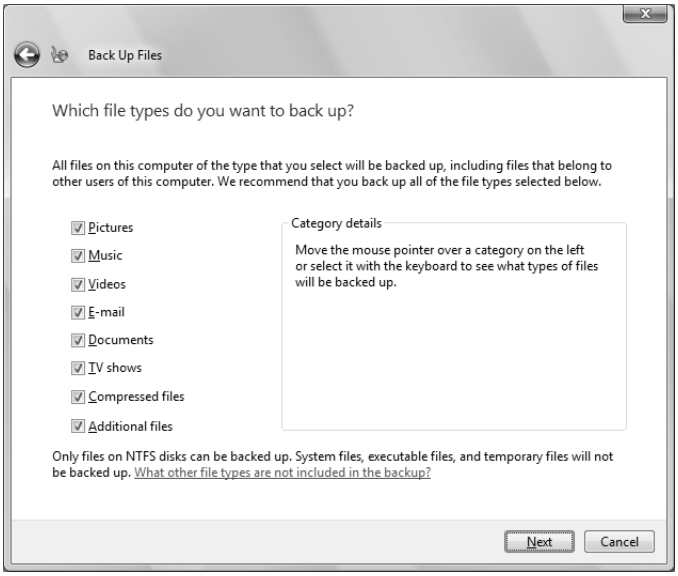
Backing Up Files

1. Select Start ➢ All Programs ➢ Maintenance ➢ Backup and Restore Center.
2. Click the Back Up Files button.
3. Select the location where you want to save your backup, then click Next.

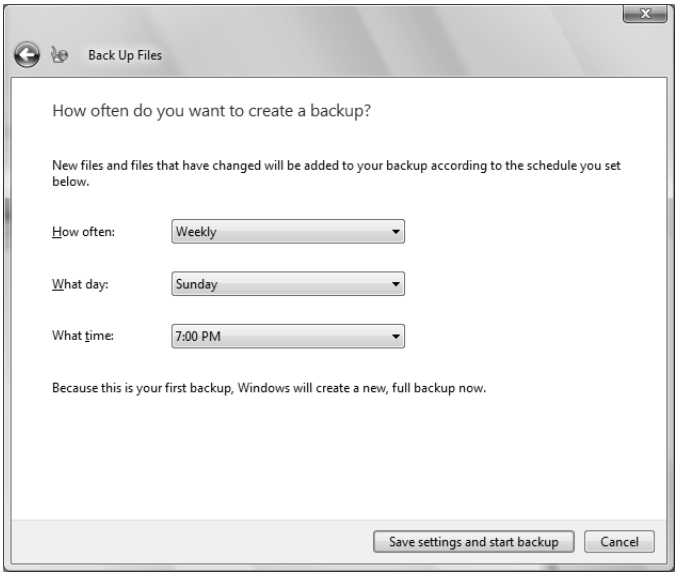


EXERCISE 11.13 *(continued)*

4. Select the files you want to back up, then click Next.

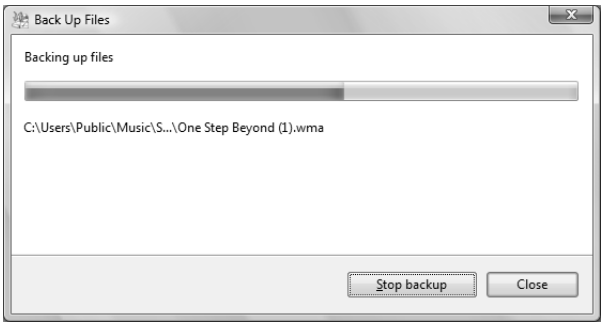


5. Select how often you want a backup to be automatically performed. To start the backup, click the Save Settings and Start Backup button.



EXERCISE 11.13 *(continued)*

6. Windows will begin backing up files, and a progress indicator will indicate how the backup is progressing.



7. When the backup is complete, click Close.

Restoring Files

To restore files that have been backed up, select Restore Files. You can restore files from the latest backup or from an older backup. You can also click Advanced Restore, which will enable you to restore files from a backup made on another computer or to restore files for all users of a computer.

In Exercise 11.14, you will restore some files. This exercise assumes that you created a backup in Exercise 11.13.

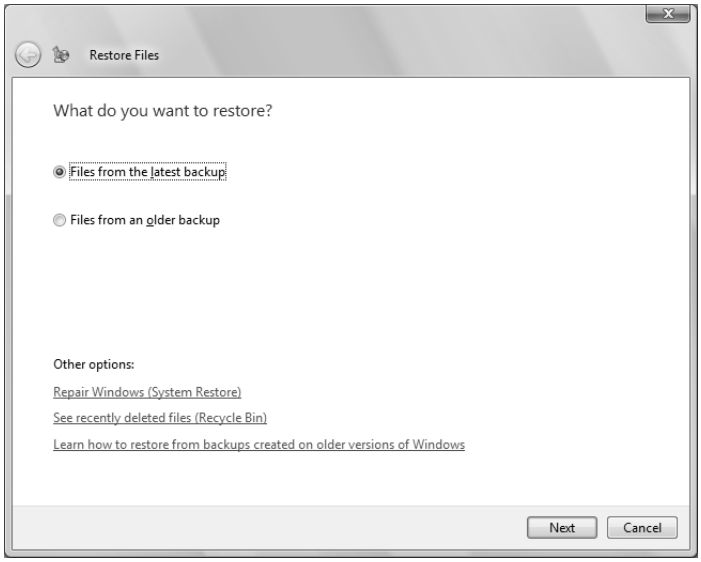
EXERCISE 11.14

Restoring Files

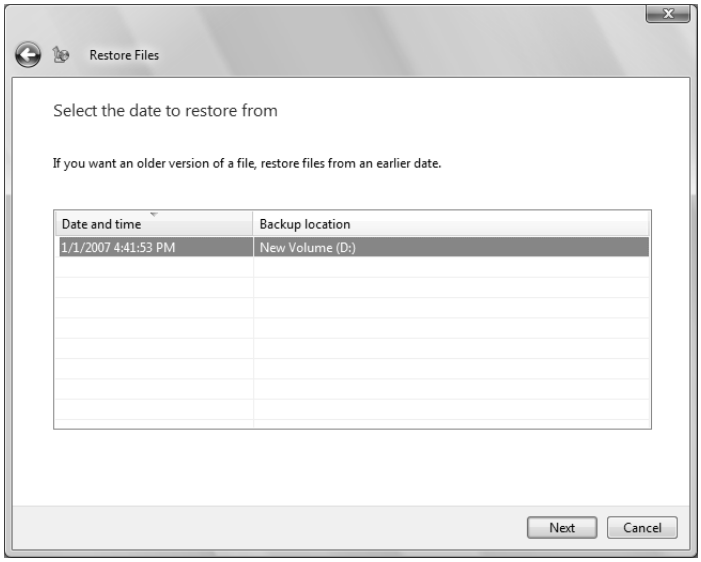
1. Select Start ➢ All Programs ➢ Maintenance ➢ Backup and Restore Center.
2. Click the Restore Files button.

EXERCISE 11.14 *(continued)*

3. Select whether you want to restore files from the latest backup or an older backup, then click Next.

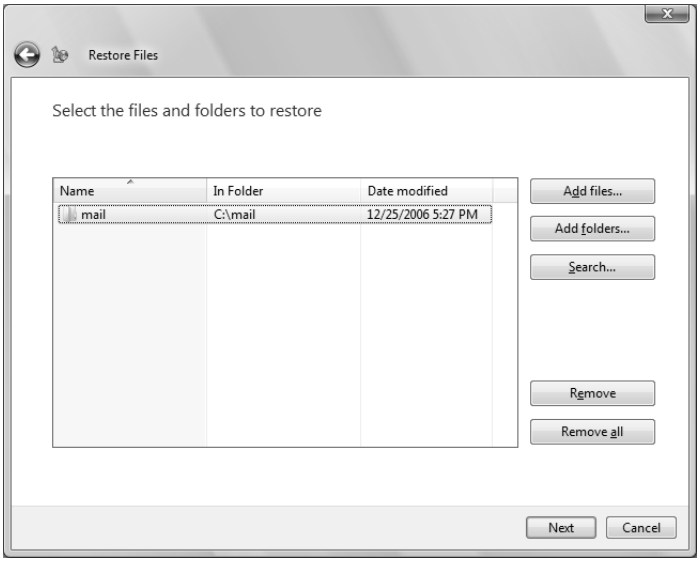


4. If you select Files from an Older Backup, you will be prompted to select the date and time of the backup. Click Next to continue.

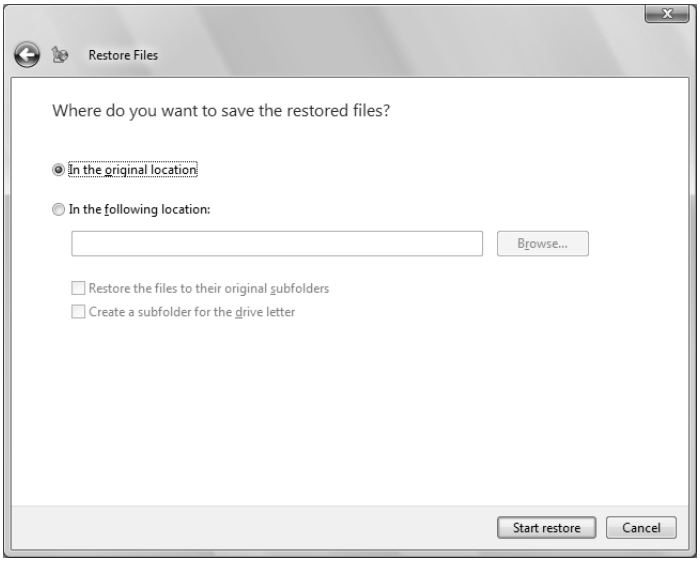


EXERCISE 11.14 *(continued)*

5. Select the files and folders you want to restore. Click Add Folders, select a folder to restore, and click Add. Click Next to continue.

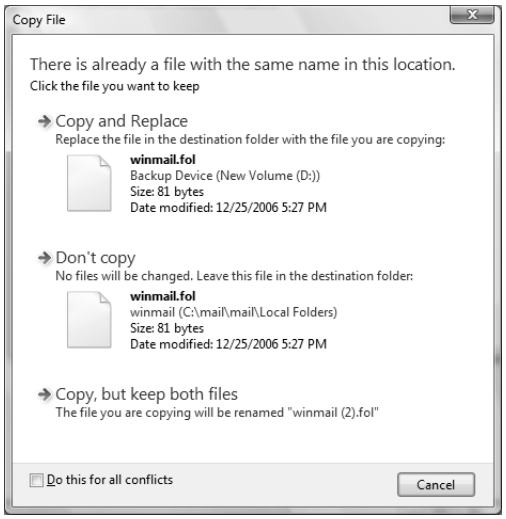


6. Select whether you want files saved in the original location or a different location. To begin the restore, select Start Restore.



EXERCISE 11.14 *(continued)*

7. If you restore a file to a location where a file already exists, you will be prompted of the conflict. Select Copy and Replace, Don't Copy, or Copy But Keep Both Files. You can also specify that your selected action be performed for all conflicts.



8. When the restore is complete, click Finish.

You can also restore files by using shadow copies. Shadow copies, which were introduced in Chapter 7, uses the backups you have created to maintain and restore previous versions of files. To restore a previous version of a file, right-click the file and select Restore Previous Versions. The Previous Versions tab of the file's Properties dialog box will appear, as shown in Figure 11.71. Click the version of the file you want to restore and click Restore.

If you restore a file to a location where a file already exists, you will be prompted of the conflict, as shown in Figure 11.72. Select Copy and Replace, Don't Copy, or Copy But Keep Both Files. You can also specify that your selected action be performed for all conflicts.

Changing Backup Settings

After you have enabled automatic backups, you can change the backup settings by clicking Change Settings. This will bring up the Backup Status and Configuration dialog box, shown in Figure 11.73. Here, you can see the status of the last backup and when the next backup will occur. You can also back up your files now by selecting Back Up Now, change your backup settings by selecting Change Backup Settings, or disable automatic backup by selecting Turn Off. If automatic backups are disabled, you can enable them by selecting Turn On.

FIGURE 11.71 File Properties, Previous Versions tab

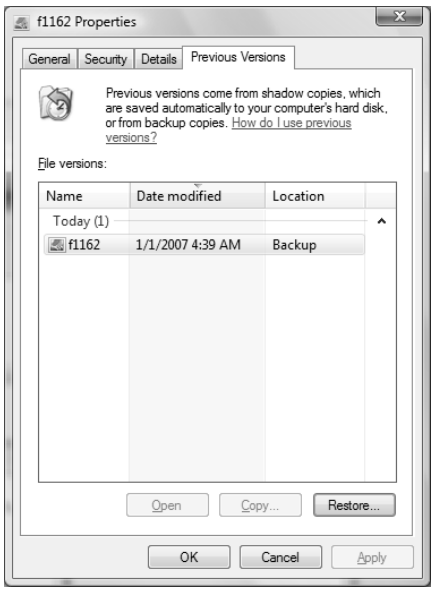


FIGURE 11.72 Copy File dialog box

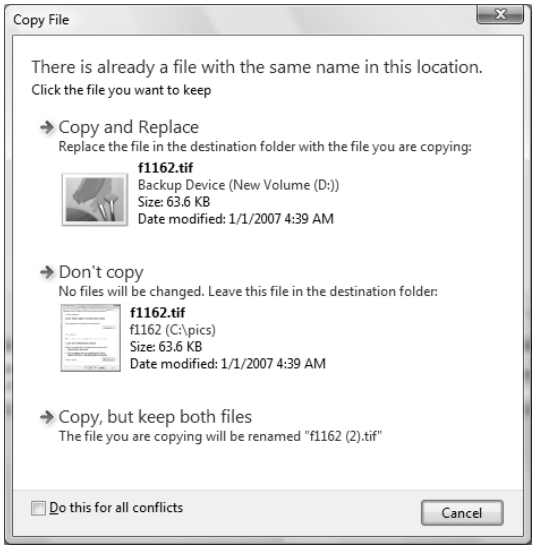
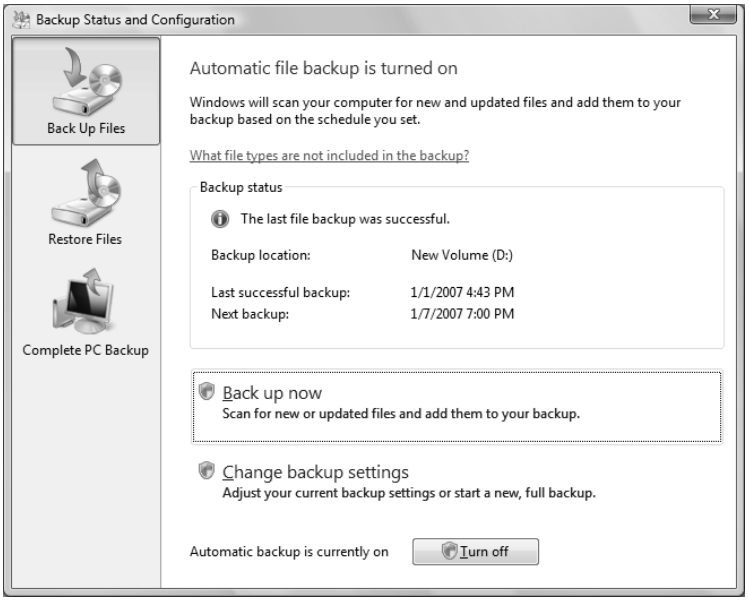


FIGURE 11.73 Backup Status and Configuration



Creating an Image

To create an image of your entire computer, select Back Up Computer. The Windows Complete PC Backup dialog box will appear, as shown in Figure 11.74. You can save the backup to a hard disk or on one or more DVDs.

You cannot save the backup to multiple CDs or a USB flash drive.

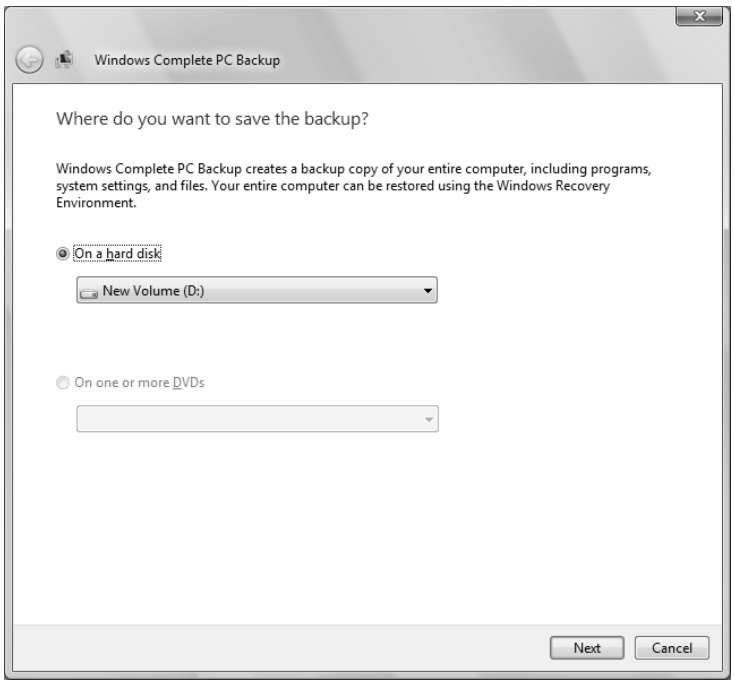
After you specify the location of the backup, Windows Complete PC Backup will let you know how large the backup might be, as shown in Figure 11.75. Click Start Backup to create the image. When the image is complete, click Close.

Restoring an Image

To restore an image, you must perform the following steps:

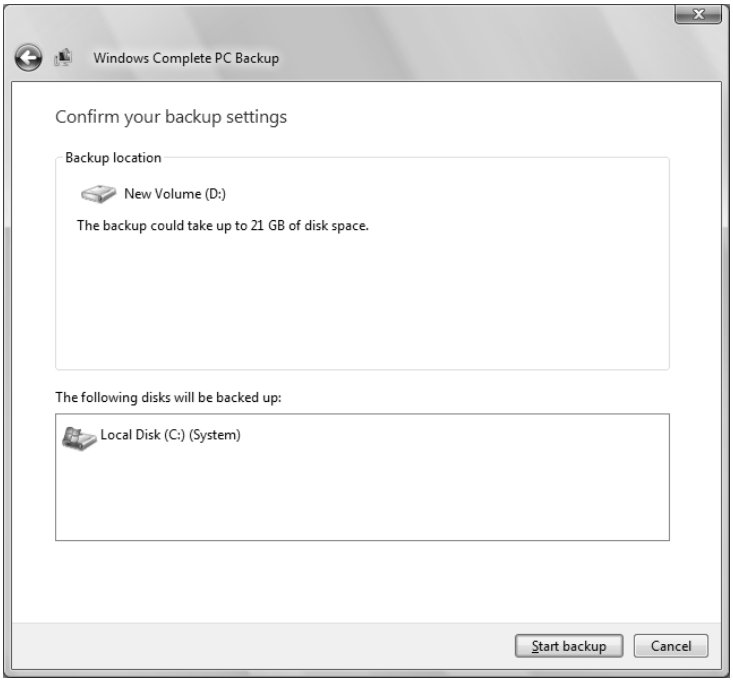
1. Boot your computer using the Windows Vista media, or use the recovery partition instructions provided by your computer manufacturer.

FIGURE 11.74 Windows Complete PC Backup



2. When the Install Windows dialog box appears, select the language, time and currency format, and the keyboard or input method. Click Next to continue.
3. The Install Now button will appear in the center of the screen. Click Repair Your Computer in the lower-left corner.
4. Select the operating system to recover and click Next. If you do not see your operating system, you might need to load your hard disk drivers by clicking the Load Drivers button.
5. The System Recovery Options dialog box will appear. You can choose one of the following options:
   - Startup Repair
   - System Restore
   - Windows Complete PC Restore
   - Windows Memory Diagnostic Tool
   - Command Prompt
6. Choose Windows Complete PC Restore to continue.

FIGURE 11.75 Confirm Your Backup Settings

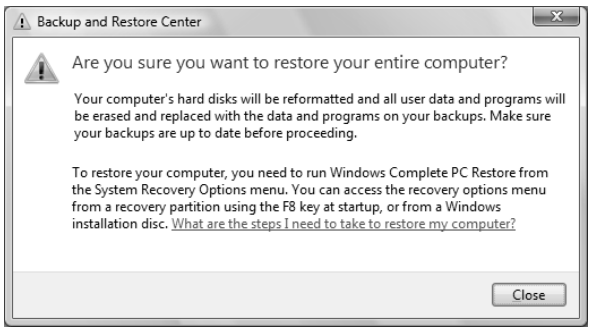


7. Select the recommended image, or select Restore a Different Backup. Click Next to continue.
8. If you selected Restore a Different Backup, follow the prompts to select the location of the image and the image you want to restore.
9. You will be asked to review your selections. Press Finish to continue.
10. You will be asked to confirm your decision. Click the check box and click OK to restore the image.

If you were not provided the Windows Vista media when you purchased your computer, the computer manufacturer might have placed the files on a recovery partition. Check with the manufacturer for more information.

If you select Restore Computer from the Backup and Restore Center, you will only be given instructions on how to restore your computer using Windows Complete PC Restore, as shown in Figure 11.76.

FIGURE 11.76 Windows Complete PC Restore



Using System Restore

System Restore monitors a computer for changes and creates restore points that can be used to restore the system files and settings on your computer to an earlier point in time without affecting your personal files. This is helpful if a virus modifies your system files, or if you install a bad driver and you want to restore the old one. When this happens, you can restore your system to a point in time before the problem first occurred.

System Restore is used for the following:

- To restore your computer to a previous state
- To restore your computer without losing personal files
- To keep dates associated with restore points
- To make restorations possible

System Restore cannot restore your personal files. To ensure your personal files are backed up, create a backup or an image of your computer.

Creating Restore Points

System Restore uses System Protection to create restore points. Restore points contain Registry and system information as they were at a certain point in time. These restore points are created at the following times:

- Every day
- Before installing applications or drivers
- Before significant system events

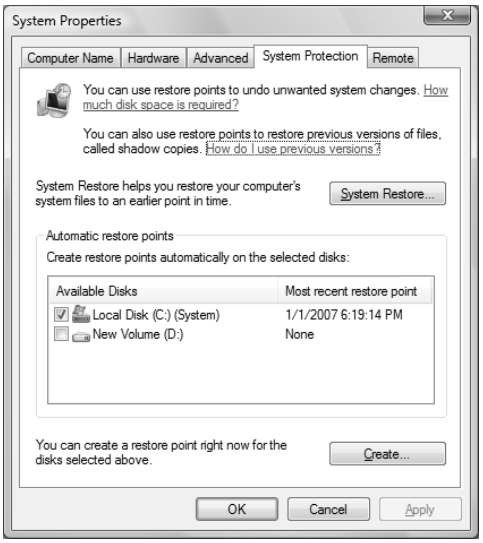
- Before System Restore is used to restore files (so that you can undo the changes if necessary)
- Manually upon request

In Exercise 11.15, we will manually create a restore point.

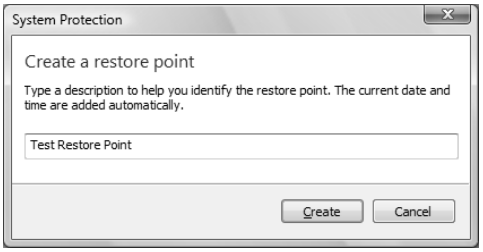
EXERCISE 11.15

Creating a Restore Point

1. Select Start ➢ All Programs ➢ Maintenance ➢ Backup and Restore Center.
2. In the left pane, click Create a Restore Point or Change Settings.
3. The System Protection tab of the System Properties dialog box will appear. Select the disks that you want to create restore points for, and click Create to create a restore point.



4. Type a description for your restore point and click Create.



5. The restore point will be created. Click OK to close the dialog box.

Restoring Restore Points

You can restore previously created restore points with System Restore. The restore operation will restore system files and settings, but will not affect your personal files.

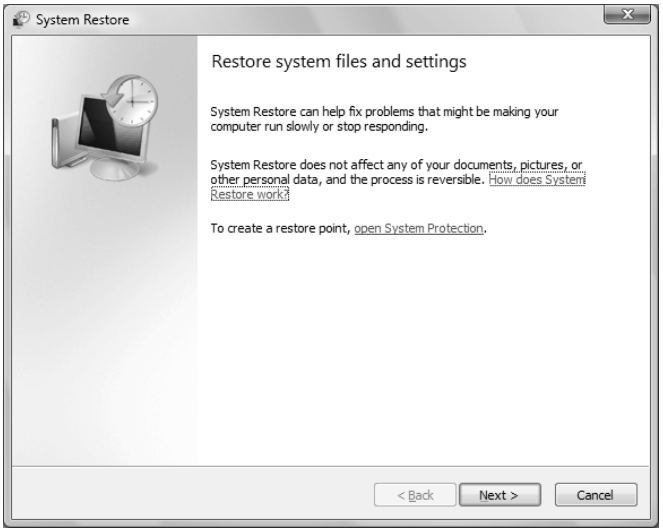
System Restore will also remove any programs that have been installed since the restore point was created.

In Exercise 11.16, we will restore a restore point.

EXERCISE 11.16

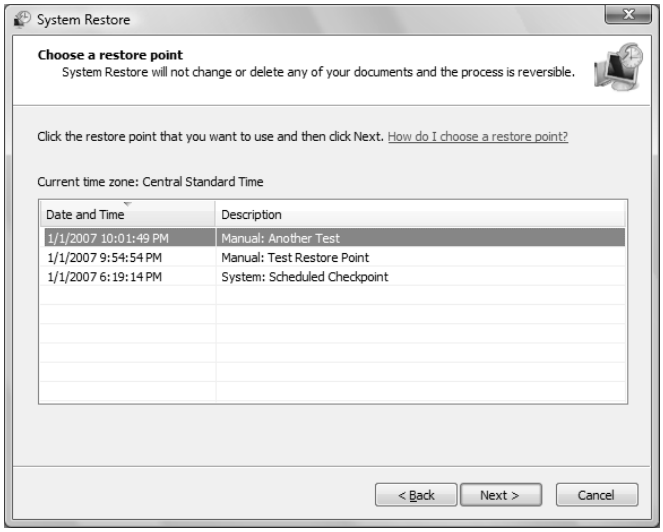
Restoring a Restore Point

1. Select Start ➢ All Programs ➢ Maintenance ➢ Backup and Restore Center.
2. In the left pane, click Repair Windows Using System Restore.
3. The System Restore dialog box will appear. Click Next to continue.

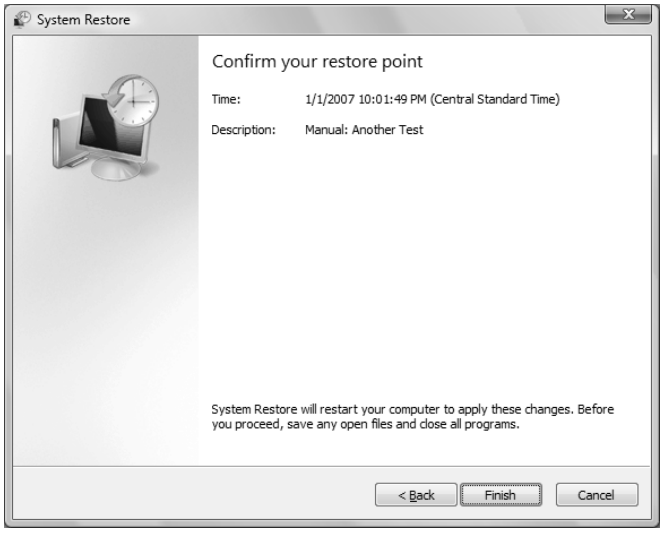


EXERCISE 11.16 *(continued)*

4. Choose a restore point, and click Next to continue.

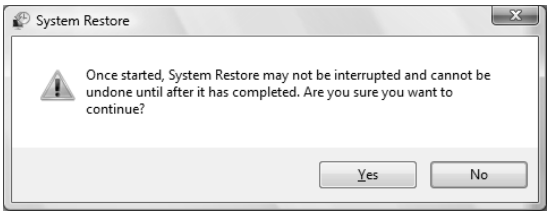


5. Review your restore point selection, and click Finish to continue.



EXERCISE 11.16 *(continued)*

6. Confirm that you want System Restore to continue, and click Yes to continue.



7. System Restore will restore your system and reboot your computer to apply the changes. You should see a message stating that System Restore has restored your computer. Click OK to close the dialog box.

If your computer will not boot, you can also perform the following steps to use System Restore:

1. Boot your computer using the Windows Vista media, or use the recovery partition instructions provided by your computer manufacturer.
2. When the Install Windows dialog box appears, select the language, time and currency format, and the keyboard or input method. Click Next to continue.
3. The Install Now button will appear in the center of the screen. Click Repair Your Computer in the lower-left corner.
4. Select the operating system to recover and click Next. If you do not see your operating system, you might need to load your hard disk drivers by clicking the Load Drivers button.
5. The System Recovery Options dialog box will appear. You can choose one of the following options:
   - Startup Repair
   - System Restore
   - Windows Complete PC Restore
   - Windows Memory Diagnostic Tool
   - Command Prompt
6. Choose System Restore to continue.
7. Follow the prompts to restore the restore point. The prompts will be similar to those in Exercise 11.16.

If you were not provided the Windows Vista media when you purchased your computer, the computer manufacturer might have placed the files on a recovery partition. Check with the manufacturer for more information.

Troubleshooting System Restore

If System Restore does not fix your problems, you can either undo the restore or attempt to restore an earlier restore point. If neither of these options works, you could try to use the Startup Repair Tool if the problem is related to missing or corrupted system files.

Summary

In this chapter, you learned about maintaining and optimizing Windows Vista. We covered the following topics:

- Using Reliability and Performance Monitor to track and monitor your system's performance
- Using Reliability Monitor to track the stability of the computer
- Monitoring and optimizing memory, the processor, the disk subsystem, and the network subsystem, and creating a system baseline
- Using the Memory Diagnostics Tool to diagnose memory problems
- Using System Information, Task Manager, and Performance Information and Tools to collect information about your system
- Using the System tool in Control Panel to optimize performance
- Using System Configuration to view and troubleshoot startup tasks
- Automating tasks through the Task Scheduler utility
- Using the Event Viewer utility, including how to view the details of an event and manage log files
- Improving file searches by using Indexing Options
- Using Remote Desktop and Remote Assistance to connect to computers remotely
- Using the Advanced Boot Options menu, including Safe Mode, Enable Boot Logging, Last Known Good Configuration, and other options
- Using the Startup Repair Tool to repair a damaged installation
- Using Backup and Restore Center to back up and restore files and to create and restore images
- Using System Protection to create checkpoints of your system configuration, and using System Restore to restore previous system configurations

Exam Essentials

Be able to monitor and troubleshoot Windows Vista performance. Know which utilities can be used to track Windows Vista performance events and issues. Know how to track and identify performance problems related to memory, the processor, the disk subsystem, and the network subsystem. Be able to correct system bottlenecks when they are identified.

Know how to use the Task Scheduler to automate system tasks. Understand the purpose of Task Scheduler. Be able to configure Task Scheduler and identify problems that would keep it from running properly.

Understand the different options for managing system recovery. Know how to use the Startup Repair Tool, System Restore, and Backup and Restore Center, and when it is appropriate to use each option.

Be able to perform file recovery with Backup and Restore Center and Shadow Copies. Understand the options that are supported through the Backup and Restore Center and the files that are backed up using this tool.

Know how to troubleshoot using Task Manager, Event Viewer, System Information, Performance Information and Tools, and Problem Reports and Solutions. Understand how to use and configure each of these tools.

Know how to troubleshoot using Advanced Boot Options. Be able to list the options that can be accessed through Advanced Boot Options, and know when it is appropriate to use each option.

Know how to use Remote Desktop and Remote Assistance. Be familiar with how Remote Desktop and Remote Assistance work and how they are configured and accessed.

Review Questions

1. You are the network administrator for the XYZ Corporation. Users in the sales department have been complaining that the Sales application is slow to load. Using Performance Logs and Alerts, you create a baseline report for one of the computers, monitoring memory, the processor, the disk subsystem, and the network subsystem. You notice that the disk subsystem has a high load of activity. What other subsystem should you monitor before you can know for sure whether you have a disk subsystem bottleneck?

   A. Memory

   B. Processor

   C. Network

   D. Application

2. You are the network administrator for a small company. You manage the computers for the marketing department, all of which are running the Windows XP Professional operating system. You are making several configuration changes to the manager's computer to enhance performance. Before you make any changes, you want to create a restore point that can be used if any problems arise. How do you manually create a restore point?

   A. By using the System Restore utility

   B. By using the System Protection tab of the System Properties dialog box

   C. By using the System Configuration utility

   D. By using the Startup Repair Tool

3. Your computer uses a SCSI adapter that supports a SCSI drive, which contains your Windows Vista system and boot partitions. After updating the SCSI driver, you restart your computer, but Windows Vista will not load. You need to get this computer up and running as quickly as possible. Which of the following repair strategies should you try first to correct your problem?

   A. Restore your computer's configuration with your last backup.

   B. Boot your computer with the Last Known Good Configuration.

   C. Boot your computer with the Safe Mode option.

   D. Boot your computer to the Recovery Console and manually copy the old driver back to the computer.

4. You are about to install a new driver for your CD-ROM drive, but you are not 100 percent sure that you are using the correct driver. Which of the following options will allow you to most easily return your computer to the previous state if the new driver is not correct?

   A. Safe Mode

   B. Roll Back Driver

   C. System Restore utility

   D. Startup Repair Tool

5. You work on the help desk for the ABC Corporation. One of your users who works remotely is having trouble getting an application you manage to work. You would like to use Remote Assistance to troubleshoot and correct the problem. The user connects to the Internet through a standard ISP connection. You connect to the Internet via a corporate network that is protected by a firewall. The firewall is not configured to use Network Address Translation (NAT). The remote user sends you a Remote Assistance invitation. When you attempt to accept the invitation, you can't connect to the remote computer. When you ping the remote user's computer, you verify that you have TCP/IP connectivity. Which of the following options should you take next?

   A. Ask the system administrator to open port 3389 on the firewall.

   B. Ask the system administrator to open port 2671 on the firewall.

   C. Verify that the remote user has your computer added the Remote Desktop Users list on the Remote tab of System Properties.

   D. Have the remote user resend the invitation and verify that the time has not expired.

6. You are the network administrator for the BrainBeacon Corporation. Your accounting manager uses a financial application that requires several hours a day to create reports that are required by the accounting department. While the application is running, the accounting manager finds that his computer is very slow when running other accounting applications. You have been asked to configure his computer so that the other accounting applications that are being run are more responsive. Which of the following configuration changes should you make?

   A. Configure the accounting applications to run at High priority.

   B. Configure the accounting applications to run at Realtime priority.

   C. Configure the financial application to run at Below Normal priority.

   D. Configure the financial application to run at Above Normal priority.

7. After you updated Stuart's computer, his system files became corrupted due to a virus and now need to be restored. Which of the following processes should you use to fix the problem?

   A. Restore a backup.

   B. Restore an image.

   C. Use the Startup Repair Tool.

   D. Boot to Safe Mode.

8. You are the network administrator for a large company. You have several remote locations that are connected via a wide area network. One of your users, Emily, calls you with an application error she is encountering. Her computer is running Windows Vista. You want to see exactly what is happening so you can help her resolve the problem. Your computer is also running Windows Vista. Which of the following options can be used to start a Remote Assistance session? (Choose all that apply.)

   A. Emily can request Remote Assistance through e-mail.

   B. Emily can request Remote Assistance by sending an instant message.

   C. As an administrator, you can offer Remote Assistance to Emily.

   D. Emily can save an invitation file on her computer and then transfer it to you.

9. When you booted Windows Vista, you noticed that an error appeared during the startup sequence. You need the exact error code that was generated, but you can't remember what the error code was. Where can you find this information?

   A. `\Windows\error.log` file

   B. `\Windows\System32\error.log` file

   C. `\Windows\System32\startup.log` file

   D. Event Viewer System log

10. You are unable to boot your Windows Vista computer, so you decide to boot the computer to Safe Mode. Which of the following statements regarding Safe Mode is false?

    A. When the computer is booted to Safe Mode, there is no network access.

    B. Safe Mode loads all the drivers for the hardware that is installed on the computer.

    C. When you run Safe Mode, boot logging is automatically enabled.

    D. When you run Safe Mode, the screen resolution is set to 800×600.

11. You have been having problems with your Windows Vista Professional computer. You decide to start the computer using the Enable Boot Logging option on the Advanced Boot Options menu. Where can you find the log file that is created?

    A. `\Windows\ntbtlog.txt`

    B. `\Windows\System32\ntbtlog.txt`

    C. `\Windows\ntboot.log`

    D. `\Windows\System32\ntboot.log`

12. Your accounting department runs a processor-intensive application and you are trying to determine whether their current computers need to have the processors upgraded. You load a test computer with a configuration identical to the production computers' and run a program that simulates a typical user's workload. You monitor the Processor > % Processor Time counter. What average value for this counter would indicate a processor bottleneck?

    A. Over 5%

    B. Over 50%

    C. Over 60%

    D. Over 85%

13. You are the network administrator for a large corporation. The accounting department requires that a specific application, `BBCASH.EXE`, be run every day to create daily reports on accounting activity. The application needs to be run at 6 PM on Monday through Friday. The accounting manager has asked you to automate the process so that reports are generated on the specified schedule without any user interaction. Which Windows Vista utility should you use?

    A. Task Scheduler

    B. Automated Scheduler

    C. Task Manager

    D. Task Automater

14. You are the network administrator for a large company. The payroll manager has Windows Vista installed on her desktop computer. The computer has the following configuration:

- Dual Pentium 4 processors
- 1GB of RAM
- Two physical SCSI disks
- Disk 0 has Partitions C: and D:
- Disk 1 has Partition E:
- 1.5GB pagefile on Partition C:
- 100Mbps Fast Ethernet NIC

The payroll manager requires the use of a database application. She has come to you to report that when the database application is running, the computer slows down very significantly, and she is unable to run any other applications. You run Reliability and Performance Monitor on her computer and record the following information when the database application is running:

- Sustained processor utilization is at 100% for both processors.
- There are a significant number of hard page faults.

When you record the data for the computer when the database application is not running, you record the following information:

- Average processor utilization is at 30%.
- There are a significant number of hard page faults.

The database application is critical to the finance manager's job. In order to be able to better manage her productivity, which two of the following actions will have the greatest impact on optimizing her computer's performance?

A. Upgrade the processors in her computer.

B. Add memory to the computer.

C. Split the page file over D: and E:.

D. Increase the page file to 3GB.

15. You have purchased a new computer with Windows Vista installed. After modifying the system so that it is configured just how you want it, you want to back up the system so that if anything happens, you can restore the files and settings. Which of the following should you do?

A. Back up your files using the Back Up Files button in Backup and Restore Center.

B. Create an image of your computer using the Back Up Computer button in Backup and Restore Center.

C. Use the System Repair Tool to take an image of your computer.

D. Use Shadow Copies to create a previous version of the files.

16. You use Remote Desktop to connect to a computer in order to change the desktop background to the standard corporate image. However, when you log on, you cannot see the desktop background. You check the Experience tab of the Remote Desktop Connection dialog box to troubleshoot. Which of the following Remote Desktop connection speeds will allow you to perform this task? (Choose all that apply.)

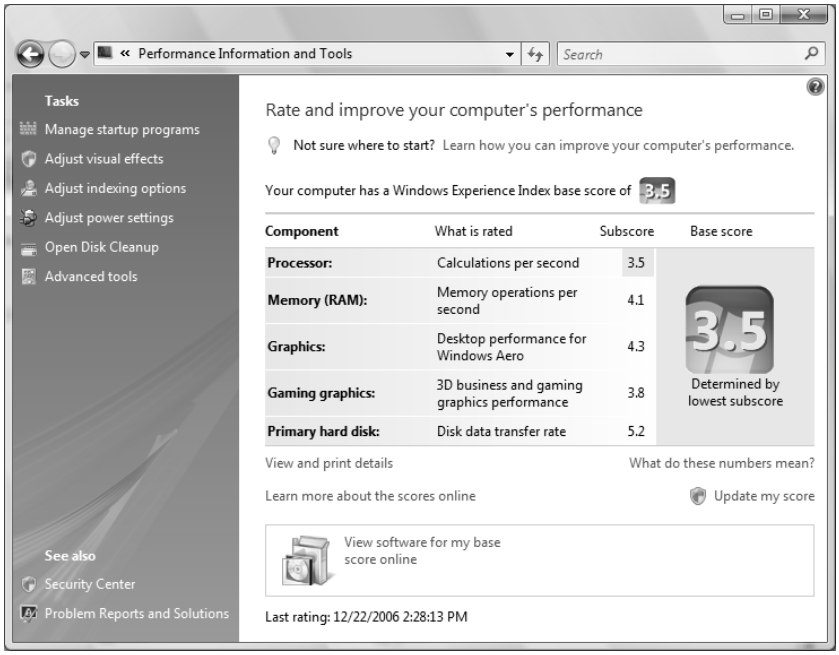
A. Modem (56.6 Kbps)

B. Broadband (128 Kbps–1.5 Mbps)

C. LAN (10 Mbps or higher)

D. Custom

17. Hayden wants to install a game on his Windows Vista computer. The game box specifies that it runs on a computer with a Windows Experience Index base score of 4.0. He runs Performance Information and tools and sees the following information:



Which of the following should Hayden do to ensure that his computer meets the minimum requirements?

A. Upgrade the memory and CPU.

B. Upgrade the memory and graphics card.

C. Upgrade the CPU and graphics card.

D. Install the application on a new computer.

18. Every time you use a device on your Windows Vista computer, it crashes and an error is displayed. You have attempted to uninstall and reinstall the driver, but the problem continues to occur. Which of the following tools should you use to search for possible fixes for your problem?

A. Dr. Watson

B. Device Manager

C. Event Viewer

D. Problem Reports and Solutions

19. You have installed Remote Desktop Web Connection on a computer that you want to access from another location. The computer can be accessed by using the fully qualified domain name aldridge.brainbeacon.com. The IP address of the computer is 10.20.30.40. What address would you use to access this computer?

A. `http://aldridge.brainbeacon.com/tsweb/`

B. `http://aldridge.brainbeacon.com/rdweb/`

C. `http://10.20.30.40/remotedesktop/`

D. `https://10.20.30.40:3389/remotedesktop/`

20. You are the administrator for a large production company. You are considering whether to use Remote Assistance to provide assistance to your users. The computers on your network run a variety of operating systems, including Windows 98, Windows 2000 Professional, Windows XP Professional, and Windows Vista Business. Which of the following operating systems can use Remote Assistance? (Choose all that apply.)

A. Windows 98

B. Windows 2000 Professional

C. Windows XP Professional

D. Windows Vista Business

Answers to Review Questions

1. A. You should check the memory counters. If your computer does not have enough memory, it can cause excessive paging, which may be perceived as a disk subsystem bottleneck.

2. B. To manually create a restore point or to restore your computer to a previous restore point, you use the System Protection tab of the System Properties dialog box. Although System Restore uses restore points, you do not use the System Restore utility to create a restore point.

3. B. If you need to get a stalled computer up and running as quickly as possible, you should start with the Last Known Good Configuration option. This option is used when you've made changes to your computer's hardware configuration and are having problems restarting. The Last Known Good Configuration will revert to the configuration used the last time the computer was successfully booted. Although this option helps overcome configuration errors, it will not help for hardware errors.

4. B. The Roll Back Driver option is the easiest way to roll back to a known good driver. You could also use the System Restore utility to roll back your computer to a known restore point if you make harmful changes to your computer, but driver rollback is easier and faster.

5. A. If you want to have access between a user from the Internet and a user who is behind a corporate firewall, then TCP port 3389 must be opened. If you do not want to open this port, then you should connect the session through VPN.

6. C. You should configure the financial application to run at Below Normal priority. This will cause the running of the financial application to have less of a performance impact on the accounting applications as they are processed.

7. C. To quickly repair the system files, you can use the Startup Repair Tool. You can restore an image using the Backup and Repair Center, but it is faster to use the Startup Repair Tool. Additionally, you will not lose any personal files by using the Startup Repair Tool. Alternatively, you could try to use System Restore to go back to a previous checkpoint.

8. A, C, D. Remote Assistance provides a mechanism for requesting help through e-mail, or by creating an invitation file and sending it manually. In addition, an administrator can offer assistance to Emily using Remote Assistance. To offer assistance, both computers must be using Windows Vista. Windows Vista no longer supports the sending of assistance requests using instant messages.

9. D. The Event Viewer utility is used to track information about your computer's hardware and software. The System log includes any error messages that have been generated.

10. B. When you run your computer in Safe Mode, you simplify your Windows Vista configuration. Only the drivers that are needed to get the computer up and running are loaded.

11. A. When you enable boot logging, the file created is `\Windows\ ntbtlog.txt`. This log file is used to troubleshoot the boot process.

12. D. If the average Processor > % Processor Time counter is consistently above 85%, a processor bottleneck may be indicated. Normally this number will spike up and down over time. If it spikes over 85%, it is not necessarily alarming. If the average is over 85%, then a bottleneck is indicated.

13. A. To automate scheduled tasks, you use Task Scheduler. You can schedule tasks to be run based on the schedule you specify and the user account that should be used to run the task.

14. A, B. The greatest improvement in performance for this computer can be obtained by upgrading the processors and adding more physical RAM. Because the database application is using 100% processor utilization over a sustained period, you need to upgrade the processors. The hard page faults indicate that you also have a memory bottleneck. While moving or increasing the page file might have an impact on performance, neither would have as large an impact as adding more physical memory will.

15. B. You should create an image of your computer using the Back Up Computer button in Backup and Restore Center. Images back up everything on your computer. File backups cannot be used to back up system files and settings.

16. C, D. You can use the LAN (10 Mbps or higher) setting or the Custom setting to enable the desktop background to be displayed. When setting the connection speed to Custom, you must manually check the box next to Desktop Background to see the desktop.

17. C. You should upgrade the CPU and graphics card to ensure that his computer meets the minimum requirements. The base score indicates the lowest scored component, not the score of all components in the computer. The two components that have scores less than 4.0 are the CPU and graphics card. All other components, including the memory, meet the game's minimum requirements.

18. D. You should use Problem Reports and Solutions to check for possible fixes for your problem. Although Device Manager and Event Viewer can provide you some helpful troubleshooting information, you cannot use them to search for solutions to your problem.

19. A. You would use the address `http://aldridge.brainbeacon.com/tsweb/` to access this computer. You can access the computer by name or by IP address. Unless you change the port, Remote Desktop Web Connection uses port 80 by default.

20. C, D. Remote Assistance requires that the computers on both sides of the connection run Windows XP Professional, Windows Server 2003, or Windows Vista. Windows 98 and Windows 2000 Professional cannot use Remote Assistance.

Glossary

# #

802.11 wireless LAN 802.11 is a wireless standard for LAN support that includes automatic wireless configuration (for zero client configuration), autodetection of wireless networks, automatic switching between different access points (APs) when a client is roaming, and wireless device authentication support for Windows Remote Authentication Dial-In User Service (RADIUS) Server and Internet Authentication Service (IAS).

A

access token An object containing the security identifier (SID) of a running process. A process started by another process inherits the starting process's access token. The access token is checked against each object's discretionary access control list (DACL) to determine whether appropriate permissions are granted to perform any requested service.

Accessibility Options Windows Vista features used to support users with limited sight, hearing, or mobility. Accessibility Options include special keyboard, sound, display, and mouse configurations.

account lockout policy A Windows Vista policy used to specify how many invalid logon attempts should be tolerated before a user account is locked out. Account lockout policies are set through account policies.

account policies Windows Vista policies used to determine password and logon requirements.

Active Directory A directory service available with the Windows 2000 Server and Windows Server 2003 platforms. Active Directory stores information in a central database and allows users to have a single user account (called a domain user account or Active Directory user account) for the network.

Active Directory user account A user account that is stored in the Windows 2000 or Windows 2003 Active Directory's central database. An Active Directory user account can provide a user with a single user account for a network. Also called a domain user account.

adapter Any hardware device that allows communications to occur through physically dissimilar systems. This term usually refers to peripheral cards that are permanently mounted inside computers and provide an interface from the computer's bus to another medium such as a hard disk or a network.

add-ons Applications that can be installed to extend the functionality of Internet Explorer.

Administrator account A Windows Vista special account that has the ultimate set of security permissions and can assign any permission to any user or group. By default, the Administrator user account is disabled.

Administrators group A Windows Vista built-in group that consists of administrative-level user accounts.

alert A system-monitoring feature that is generated by Reliability and Performance Monitor when a specific counter exceeds or falls below a specified value.

Allowed Items List in Windows Defender that contains software that has been marked as safe.

Alternate IP Configuration A feature that allows users to have a static and a DHCP-assigned IP address mapped to a single network adapter, which is often used to support users who connect to multiple locations.

Anonymous Logon group A Windows Vista special group that includes users who access the computer through anonymous logons. Anonymous logons occur when users gain access through special accounts, such as the IUSR_*computername* and TsInternetUser user accounts. Normally, a password is not required, so that anyone can log on.

answer files An automated installation script used to respond to configuration prompts that normally occur in a Windows Vista installation. Administrators can create answer files with the Windows System Image Manager utility.

APIPA See Automatic Private IP Addressing.

Application log A log that tracks events that are related to applications that are running on the computer. The Application log can be viewed in the Event Viewer utility.

audit policy A Windows Vista policy that tracks the success or failure of specified security events. Audit policies are set through the Local Computer Policy snap-in.

Authenticated Users group A Windows Vista special group that includes users who access the Windows Vista operating system through a valid username and password.

authentication The process required to log on to a computer locally. Authentication requires a valid username and a password that exists in the local accounts database. An access token will be created if the information presented matches the account in the database.

Authentication is also used when you access a network through a dial-up connection, virtual private network (VPN), or direct connection. Windows Vista uses a two-step authentication process, which consists of an interactive logon process and network authorization. The interactive logon process confirms a user's identity based on the user account (local or domain) and password or smart card credentials. Network access control is used to confirm the user's identity to the network service or resource that the user is attempting to access.

automated installation The process of installing Windows Vista using an unattended setup method such as Windows Deployment Services (WDS), or unattended installation.

Automatic Private IP Addressing (APIPA) A service that is used to automatically assign private IP addresses for home or small business networks that contain a single subnet, have no DHCP server, and are not using static IP addressing. If APIPA is being used, then clients will

be able to communicate only with other clients on the same subnet that are also using APIPA. The benefit of using APIPA in small networks is that it is less tedious and has less chance of configuration errors than statically assigned IP addresses and configuration.

B

backup The process of writing all the data contained in online mass-storage devices to offline mass-storage devices for the purpose of safekeeping. Backups are usually performed from hard disk drives to tape drives, network locations, or other hard disk drives. Also referred to as archiving.

Backup and Restore Center A Windows Vista utility that allows you to create and restore backups and images.

Backup Operators group A Windows Vista built-in group that includes users who can back up and restore the file system, even if the file system is NTFS and they have not been assigned permissions to the file system. The members of the Backup Operators group can access the file system only through the Backup utility. To be able to directly access the file system, the user must have explicit permissions assigned.

Balanced power plan A power plan included with Windows Vista that provides a balance between power savings and performance. The Balanced power plan can be customized to suit the needs of the user.

baseline A snapshot record of a computer's current performance statistics that can be used for performance analysis and planning purposes.

basic storage A disk-storage system supported by Windows Vista that consists of primary partitions and extended partitions.

battery meter A Windows Vista utility that monitors battery power consumption on laptop computers.

Basic Input/Output System (BIOS) A set of routines in firmware that provides the most basic software interface drivers for hardware attached to the computer. The BIOS contains the boot routine.

BCD store See Boot Configuration Data store.

BCDEdit A utility that enables you to edit the boot options in the BCD store.

BIOS See Basic Input/Output System.

BitLocker Drive Encryption Utility in Windows Vista Enterprise and Windows Vista Ultimate that is used to encrypt information on the drive that contains your operating system.

Bluetooth A short-range radio technology that simplifies communication between local computer devices and external devices.

boot The process of loading a computer's operating system. Booting usually occurs in multiple phases, each successively more complex until the entire operating system and all its services are running. Also called bootstrap. The computer's BIOS must contain the first level of booting.

Boot Configuration Data (BCD) store Contains dual-boot and multiboot information parameters that were previously found in `boot.ini` in older versions of Windows. The BCD store is new to Windows Vista.

boot partition The partition that contains the system files. The system files are located in `C:\Windows` by default.

bottleneck A system resource that is inefficient compared with the rest of the computer system as a whole. The bottleneck can cause the rest of the system to run slowly.

C

central processing unit (CPU) The main processor in a computer.

certificate authentication A security authentication process that uses a special authentication credential, called a certificate. A certificate is a digital signature that is issued by a certificate authority. When a client and server are configured to use certificate authentication, they must both present a valid certificate for mutual authentication.

Challenge Handshake Authentication Protocol (CHAP) A security protocol used to negotiate secure authentication by using encryption that is based on the industry standard hashing scheme specified by Message Digest 5 (MD5). Hashing schemes are used to transform data into a scrambled format. CHAP uses a challenge-response process that sends the client a request with the hash scheme that will be used. The client then responds to the server with an MD5 hashed response. This method allows the server to authenticate a client without the client actually sending their password over the remote connection. Almost all third-party Point-to-Point Protocol (PPP) servers support CHAP authentication.

CHAP See Challenge Handshake Authentication Protocol.

Check Disk utility A Windows Vista utility that checks a hard disk for errors. Check Disk (chkdsk) attempts to fix file-system errors and scans for and attempts to recover bad sectors.

Cipher A command-line utility that can be used to encrypt and decrypt files on NTFS volumes.

cipher text Encrypted data. Encryption is the process of translating data into code that is not easily accessible. Once data has been encrypted, a user must have a password or key to decrypt the data. Unencrypted data is known as plain text.

clean install A method of Windows Vista installation that puts the operating system into a new folder and uses its default settings the first time the operating system is loaded.

clear text Data or text that has not been encrypted. Also called plain text.

client A computer on a network that subscribes to the services provided by a server.

compression The process of storing data in a form using special algorithms that takes less space than the uncompressed data.

Computer The folder used to view and manage a computer. The Computer folder provides access to all local and network drives.

Computer Management A consolidated tool for performing common Windows Vista management tasks. The interface is organized into three main areas of management: System Tools, Storage, and Services and Applications.

computer name A NetBIOS name used to uniquely identify a computer on the network. A computer name can be from 1 to 15 characters long.

Control Panel A Windows Vista utility that allows users to change default settings for operating system services to match their preferences. The Registry contains the Control Panel settings.

Convert A command-line utility used to convert a partition or volume from FAT32 to NTFS.

counter A performance-measuring tool used to track specific information regarding a system resource, called a performance object. All Windows Vista system resources are tracked as performance objects, such as Cache, Memory, Paging File, Process, and Processor. Each performance object has an associated set of counters. Counters are set through the Reliability and Performance Monitor utility.

CPU See central processing unit.

Creator Group The Windows Vista special group that created or took ownership of the object (rather than an individual user). When a regular user creates an object or takes ownership of an object, the username becomes the Creator Owner group. When a member of the Administrators group creates or takes ownership of an object, the Administrators group becomes the Creator group.

Creator Owner group The Windows Vista special group that includes the account that created or took ownership of an object. The account, usually a user account, has the right to modify the object but cannot modify any other objects that were not created by the user account.

Critical event An Event Viewer event type that indicates the occurrence of an error of the highest severity.

D

DACL See discretionary access control list.

data compression The process of storing data in a form using special algorithms that takes less space than the uncompressed data.

data encryption The process of translating data into code that is not easily accessible to increase security. Once data has been encrypted, a user must have a password or key to decrypt the data. Data encryption adds an additional layer of security in remote communications, by encrypting all of the data that is sent and adding security to the logon authentication process.

Data Execution Prevention (DEP) A feature introduced in Windows XP Service Pack 2 that helps prevent damage to the operating system and applications from viruses and security threats by monitoring how programs access and use system memory.

Debugging mode A Windows Vista Advanced Boot Option menu item that runs the Kernel Debugger, if that utility is installed. The Kernel Debugger is an advanced troubleshooting utility.

default gateway A TCP/IP configuration option that specifies the gateway that will be used if the network contains routers.

DEP See Data Execution Prevention (DEP).

Desktop A directory that the background of the Windows Explorer shell represents. By default, the Desktop includes objects that contain the local storage devices and available network shares. Also a key operating part of the Windows Vista graphical interface.

device driver Software that allows a specific piece of hardware to communicate with the Windows Vista operating system.

Device Manager A Windows Vista utility used to view information about the computer's configuration and set configuration options.

DHCP See Dynamic Host Configuration Protocol.

DHCP server A server configured to provide DHCP clients with all of their IP configuration information automatically.

dial-up modem Hardware used for remote communication that uses slow links and uses an analog dial-up connection over the Public Switched Telephone Network (PSTN), which is regular phone service, for remote connectivity. It is the least expensive and most commonly used method for creating remote connections.

dial-up networking A service that allows remote users to dial in to the network or the Internet (such as through a telephone or an ISDN connection).

Digital Rights Management (DRM) A content protection mechanism used by content providers to control how and where digital music and videos can be played, burned, or synchronized to another device.

Digital Video Disc (DVD) A disk standard that supports 4.7GB of data per disk. One of DVD's strongest features is backward compatibility with CD-ROM technology, so that a DVD drive can play CD-ROMs. Formerly known as Digital Video Disk.

Disable Automatic Restart on System Failure A Windows Vista Advanced Boot Option menu item that prevents Windows from restarting when a critical error causes Windows to

fail. This option should be used only when Windows fails every time you restart so that you are not able to access the desktop or any configuration options.

Disable Driver Signature Enforcement A Windows Vista Advanced Boot Option menu item that allows drivers to be installed even if they do not contain valid signatures.

discretionary access control list (DACL) An item used by the operating system to determine resource access. Each object (such as a folder, network share, or printer) in Windows Vista has a DACL. The DACL lists the security identifiers (SIDs) contained by objects. Only the users or groups identified in the list as having the appropriate permission can activate the services of that object.

Disk Cleanup A Windows Vista utility used to identify files that can be deleted to free additional hard disk space. Disk Cleanup works by identifying temporary files, Internet cache files, and unnecessary program files.

disk defragmentation The process of rearranging the existing files on a disk so that they are stored contiguously, which optimizes access to those files.

Disk Defragmenter A Windows Vista utility that performs disk defragmentation.

disk image (disk imaging) An exact duplicate of a hard disk, used for automated installation. The disk image is copied from a reference computer that is configured in the same manner as the computers on which Windows Vista will be installed.

Disk Management utility A Windows Vista graphical tool for managing disks, partitions, and volumes.

disk partitioning The process of creating logical partitions on the physical hard drive.

distribution server A network server that contains the Windows Vista image files to be used for distributing Windows Vista remotely. Clients can connect to the distribution server and install Windows Vista over the network.

DNS See Domain Name System.

Documents The default storage location for documents that are created. Each user has a unique Documents folder.

domain In Microsoft networks, an arrangement of client and server computers referenced by a specific name that shares a single security permissions database. On the Internet, a domain is a named collection of hosts and subdomains, registered with a unique name by the InterNIC.

domain name A name that identifies one or more IP addresses, such as sybex.com. Domain names are used in URLs to identify particular web hosts.

Domain Name System (DNS) The TCP/IP network service that translates fully qualified domain names (or host names) into IP addresses.

Domain Name System (DNS) server An Internet host dedicated to the function of translating fully qualified domain names into IP addresses.

domain user account A user account that is stored in the Windows 2000 Server or Windows Server 2003 Active Directory's central database. A domain user account can provide a user with a single user account for a network. Also called an Active Directory user account.

drive letter A single letter assigned as an abbreviation to a mass-storage volume available to a computer.

driver A program that provides a software interface to a hardware device. Drivers are written for the specific devices they control, but they present a common software interface to the computer's operating system, allowing all devices of a similar type to be controlled as if they were the same.

driver rollback An option that allows you to restore a previously used driver after a driver has been upgraded. This option provides an easy mechanism for restoring a driver if the upgraded driver does not work properly.

driver signing A digital imprint that is Microsoft's way of guaranteeing that a driver has been tested and will work with the computer.

DRM See Digital Rights Management (DRM)

dual-booting The process of allowing a computer to boot two operating systems.

DVD See Digital Video Disc.

dynamic disk A Windows Vista disk-storage technique. A dynamic disk is divided into dynamic volumes. Dynamic volumes cannot contain partitions or logical drives, and they are not accessible through DOS. You can size or resize a dynamic disk without restarting Windows Vista. Dynamic disks are accessible only to Windows 2000, Windows XP, Windows Server 2003, and Windows Vista computers.

Dynamic Host Configuration Protocol (DHCP) A method of automatically assigning IP addresses to client computers on a network.

dynamic storage A Windows Vista disk-storage system that is configured as volumes. Windows Vista dynamic storage supports simple volumes, spanned volumes, and striped volumes.

E

EAP See Extensible Authentication Protocol.

EB See exabyte.

effective rights The rights that a user actually has to a file or folder. To determine a user's effective rights, add all of the permissions that have been allowed through the user's assignments based on that user's username and group associations. Then subtract any permissions that have been denied the user through the username or group associations.

EFS See Encrypting File System.

Enable Boot Logging option A Windows Vista Advanced Boot Options menu item that is used to create a log file that tracks the loading of drivers and services.

Enable Low-Resolution Video (640×480) option A Windows Vista Advanced Boot Options menu item that loads a standard VGA driver at 640 × 480 resolution without starting the computer in Safe Mode.

Encrypting File System (EFS) The Windows Vista technology used to store encrypted files on NTFS partitions. Encrypted files add an extra layer of security to the file system.

encryption The process of translating data into code that is not easily accessible to increase security. Once data has been encrypted, a user must have a password or key to decrypt the data.

Error event An Event Viewer event type that indicates the occurrence of an error, such as a driver failing to load.

Ethernet The most popular Data Link layer standard for local area networking. Ethernet implements the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) method of arbitrating multiple computer access to the same network. This standard supports the use of Ethernet over any type of media, including wireless broadcast. Standard Ethernet operates at 10Mbps. Fast Ethernet operates at 100Mbps. Gigabit Ethernet operates at 1000Mbps.

Event Viewer A Windows Vista utility that tracks information about the computer's hardware and software, as well as security events. This information is stored in several log files.

Everyone A Windows Vista special group that includes anyone who could possibly access the computer. The Everyone group includes all of the users (including Guests) who have been defined on the computer.

exabyte A computer storage measurement equal to 1,024 petabytes.

extended partition In basic storage, a logical drive that allows you to allocate the logical partitions however you wish. Extended partitions are created after the primary partition has been created.

Extensible Authentication Protocol (EAP) A remote access protocol used for logon authentication. EAP extends the services of Point-to-Point Protocol (PPP) by providing more updated and secure authentication services than were previously available with PPP. EAP was designed to provide secure authentication services for third-party (non-Microsoft) devices.

F

Failure Audit event An Event Viewer entry that indicates the occurrence of an event that has been audited for failure, such as a failed logon when someone presents an invalid username and/or password.

FAT16 The 16-bit version of the File Allocation Table (FAT) system, which was widely used by DOS and Windows 3.*x*. The file system is used to track where files are stored on a disk. Most operating systems support FAT16.

FAT32 The 32-bit version of the File Allocation Table (FAT) system, which is more efficient and provides more safeguards than FAT16. Windows 95 OSR2 and higher versions of Windows support FAT32.

fault tolerance Any method that prevents system failure by tolerating single faults, usually through hardware redundancy.

Favorites Center A feature of Internet Explorer that provides access to saved RSS feeds, history information, and the Favorites list.

File Allocation Table (FAT) The file system used by MS-DOS and available to other operating systems such as Windows (all versions) and OS/2. FAT has become something of a mass-storage compatibility standard because of its simplicity and wide availability. FAT has fewer fault-tolerance features than the NTFS file system and can become corrupted through normal use over time.

file attributes Information stored along with the name and location of a file in a directory entry. File attributes show the status of a file, such as archived, hidden, and read-only. Different operating systems use different file attributes to implement services such as sharing, compression, and security.

file system A software component that manages the storage of files on a mass-storage device by providing services that can create, read, write, and delete files. File systems impose an ordered database of files on the mass-storage device. Storage is arranged in volumes. File systems use hierarchies of directories to organize files.

File Transfer Protocol (FTP) A simple Internet protocol that transfers complete files from an FTP server to a client running the FTP client. FTP provides a simple, low-overhead method of transferring files between computers but cannot perform browsing functions. Users must know the URL of the FTP server to which they wish to attach.

firewall Combination of hardware and software that is used to provide security between an internal network or intranet or a remote client and the Internet. The use of a firewall prevents unauthorized access by preventing direct communication between a computer behind the firewall and the Internet via a proxy server.

fragmentation A process that naturally occurs as users create, delete, and modify files. The access of noncontiguous data is transparent to the user; however, when data is stored in this manner, the operating system must search through the disk to access all the pieces of a file. This slows down data access.

Frame Relay A technology that uses a virtual circuit–based switching protocol to connect devices on a WAN. Frame Relay is commonly implemented with a permanent virtual circuit.

FTP See File Transfer Protocol.

G

gadgets Small applications used by Windows Sidebar that provide quick, visual representations of information.

GB See gigabyte.

GHz See gigahertz (GHz).

gigabyte A computer storage measurement equal to 1,024 megabytes.

gigahertz (GHz) One billion cycles per second. The internal clock speed of a microprocessor is expressed in megahertz (MHz) or gigahertz (GHz).

GPO See Group Policy Object.

Graphic Device Interface (GDI) The programming interface and graphical services provided to Windows Vista for programs to interact with graphical devices such as the screen and printer.

Graphical User Interface (GUI) A computer shell program that represents mass-storage devices, directories, and files as graphical objects on a screen. A cursor driven by a pointing device such as a mouse manipulates the objects.

Group Policy Object (GPO) An option for managing configuration settings that comprises Windows Vista configuration settings, administered through the use of Group Policy Objects (GPOs). GPOs are data structures that are attached in a specific hierarchy to selected Active Directory Objects. You can apply GPOs to sites, domains, or organizational units.

Group Policy Object Editor snap-in A Microsoft Management Console (MMC) snap-in used to implement group policies, which include computer configuration policies and user configuration policies.

Group Policy Result Tool A tool used to help determine which policies will actually be applied. This tool is accessed through the `GPResult.exe` command-line utility. The `gpresult` command displays the resulting set of policies that were enforced on the computer and the specified user during the logon process.

groups Security entities to which users can be assigned membership for the purpose of applying a broad set of group permissions to the user. By managing permissions for groups and assigning users to groups, rather than assigning permissions to users, administrators can more easily manage security.

Guest account A Windows Vista user account created to provide a mechanism to allow users to access the computer even if they do not have a unique username and password. This account normally has very limited privileges on the computer. This account is disabled by default.

Guests group A Windows Vista built-in group that has limited access to the computer. This group can access only specific areas. Most administrators do not allow Guest account access because it poses a potential security risk. This group is disabled by default.

GUI See Graphical User Interface.

H

hard disk drive A mass-storage device that reads and writes digital information magnetically on disks that spin under moving heads. Hard disk drives are precisely aligned and cannot normally be removed, except for maintenance. Hard disk drives are an inexpensive way to store gigabytes of computer data permanently. Hard disk drives also store the software installed on a computer.

hibernation The process of storing anything that is in memory on the computer's hard disk. Hibernation ensures that none of the information stored in memory is lost when the computer is put in low-power mode. When the computer is taken out of hibernation, it is returned to its previous state.

High Performance power plan A power plan included with Windows Vista that is optimized for computer performance rather than power savings.

home folder A folder where users normally store their personal files and information. A home folder can be a local folder or a network folder.

HTML See Hypertext Markup Language.

HTTP See Hypertext Transfer Protocol.

hyperlink A link within text or graphics that has a web address embedded in it. By clicking the link, a user can jump to another web address.

Hypertext Markup Language (HTML) A textual data format that identifies sections of a document such as headers, lists, hypertext links, and so on. HTML is the data format used on the World Wide Web for the publication of web pages.

Hypertext Transfer Protocol (HTTP) An Internet protocol that transfers HTML documents over the Internet and responds to context changes that happen when a user clicks a hyperlink.

I

ICACLS A command-line tool that is used to view effective permissions in Windows Vista.

IE See Internet Explorer.

ImageX A Windows Vista command-line utility used to create disk images.

IMAP See Internet Message Access Protocol

inbound rule A Windows Firewall rule that applies to network traffic coming into the computer.

Indexing Options A Windows Vista tool that creates an index based on the contents and properties of files stored on the computer's local hard drive. A user can then use the Windows Vista Search function to search or query through the index for specific keywords.

Information event An Event Viewer entry that informs you that a specific action has occurred, such as when a system shuts down or starts.

inherited permissions Parent folder permissions that are applied to (or inherited by) files and subfolders of the parent folder. In Windows Vista, the default is for parent folder permissions to be applied to any files or subfolders in that folder.

initial user account The account that uses the name of the first registered user. By default, the initial user is a member of the Administrators group.

Instant Search A feature of Internet Explorer that displays a search bar on the IE toolbar, which allows you to quickly and easily search for a phrase using the search providers that have been configured.

Integrated Services Digital Network (ISDN) Provides digital telephone service. In order to use ISDN, an ISDN line must be installed and configured by the remote client and the server site. Basic-rate ISDN lines can support transmissions of up to 128Kbps (kilobits per second) and use two 64Kbps channels. ISDN normally uses a dial-up connection, rather than a permanent connection.

Interactive group A Windows Vista special group that includes all the users who use the computer's resources locally.

interactive logon A logon when the user logs on from the computer where the user account is stored on the computer's local database. Also called a local logon.

interactive user A user who physically logs on to the computer where the user account resides (rather than logging on over the network).

Internet Explorer (IE) A World Wide Web browser produced by Microsoft and included with all Windows operating systems.

Internet Message Access Protocol (IMAP or IMAP4) A protocol used to receive e-mail messages over the Internet.

Internet Protocol (IP) The Network layer protocol upon which the Internet is based. IP provides a simple connectionless packet exchange. Other protocols such as TCP use IP to perform their connection-oriented (or guaranteed delivery) services.

Internet Protocol Security (IPSec) A remote data encryption standard that uses Data Encryption Standard (DES) encryption, which is a suite of cryptography-based security protocols. IPSec uses computer-level authentication and provides data encryption services for Layer Two Tunneling Protocol (L2TP) and virtual private network (VPN) connections. IPSec services include packet data authentication, data integrity, replay protection, and data confidentiality services. Point-to-Point Tunneling Protocol (PPTP) provides only packet data confidentiality services.

Internet service provider (ISP) A company that provides dial-up connections to the Internet.

internetwork A network made up of multiple network segments that are connected with some device, such as a router. Each network segment is assigned a network address. Network layer protocols build routing tables that are used to route packets through the network in the most efficient manner.

invitation A method by which a user requests another user's assistance using Remote Assistance. By default, invitations are valid for six hours.

IP See Internet Protocol.

IP address A four-byte number that uniquely identifies a computer on an IP internetwork.

ipconfig A command used to display the computer's IP configuration.

IPSec See Internet Protocol Security.

ISDN See Integrated Services Digital Network.

K

KB See kilobyte.

kernel The core process of a preemptive operating system, consisting of a multitasking scheduler and the basic security services. Depending on the operating system, other services such as virtual memory drivers may be built into the kernel. The kernel is responsible for managing the scheduling of threads and processes.

kilobyte A computer storage measurement equal to 1,024 bytes.

L

L2TP See Layer Two Tunneling Protocol.

LAN See local area network.

Last Known Good Configuration option A Windows Vista Advanced Boot Options menu item used to load the control set that was used the last time the computer was successfully booted.

Layer Two Tunneling Protocol (L2TP) An industry-standard VPN protocol that is used in conjunction with IP security (IPSec) to provide a high level of security when sending IP packets over the Internet or other public IP network. L2TP and IPSec provide data authentication, data encryption, and data integrity services that strengthen security when data is sent over an unsecured network.

lease Used by Dynamic Host Configuration Protocol (DHCP) to allow a device to use an IP address for a set period of time.

LGPO See Local Group Policy Object.

local area network (LAN) An access standard that is used to provide connectivity in a local corporate or home environment.

Local Computer Policy snap-in A Microsoft Management Console (MMC) snap-in used to implement local group policies, which include computer configuration policies and user configuration policies.

local group A group that is stored on the local computer's accounts database. These are the groups that administrators can add users to and manage directly on a Windows Vista computer.

local group policies A combination of security settings that are used to specify the levels of security defined on a Windows Vista computer.

Local Group Policy Object (LGPO) A set of security configuration settings that are applied to users and computers. LGPOs are created and stored on the Windows Vista computer.

local policies Policies that allow administrators to control what a user can do after logging on. Local policies include audit policies, security option policies, and user right policies. These policies are set through Local Computer Policy snap-in.

local security Security that governs a local or interactive user's ability to access locally stored files. Local security can be set through NTFS permissions.

local user account A user account stored locally in the user accounts database of a computer that is running Windows Vista.

local user profile A profile created the first time a user logs on, stored in the Documents and Settings folder. The default user profile folder's name matches the user's logon name. This folder contains a file called `NTUSER.DAT` and subfolders with directory links to the user's Desktop items.

Local Users and Groups A utility that is used to create and manage local user and group accounts.

locale settings Settings for regional items, including numbers, currency, time, date, and input locales.

logical drive An allocation of disk space on a hard drive, using a drive letter. For example, a 50GB logical drive could be partitioned into two logical drives: a C: drive, which might be 20GB, and a D: drive, which might be 30GB.

logoff The process of closing an open session with a Windows Vista computer or Windows domain.

logon The process of opening a session with a Windows Vista computer or a network by providing a valid authentication consisting of a user account name and a password. After logon, network resources are available to the user according to the user's assigned permissions.

logon script A command file that automates the logon process by performing utility functions such as attaching to additional server resources or automatically running different programs based on the user account that established the logon.

M

Magnifier A utility used to create a separate window to magnify a portion of the screen. This option is designed for users who have poor vision.

mandatory profile A user profile created by an administrator and saved with a special extension (.man) so that the user cannot modify the profile in any way. Mandatory profiles can be assigned to a single user or a group of users.

mapped drive A shared network folder associated with a drive letter. Mapped drives appear to users as local connections on their computers and can be accessed through a drive letter using My Computer.

Master Boot Record (MBR) A record used in the Windows Vista boot sequence to point to the active partition, which is the partition used to boot the operating system. This is normally the C: drive. Once the MBR locates the active partition, the boot sector is loaded into memory and executed.

MB See megabyte.

MBR See Master Boot Record.

MCE device See Media Center Extender device

Media Center Extender (MCE) device A device that enables you to watch or record TV, watch videos, listen to music, and view pictures without being at a computer.

megabyte A computer storage measurement equal to 1,024 kilobytes.

megahertz One million cycles per second. The internal clock speed of a microprocessor is expressed in megahertz (MHz) or gigahertz (GHz).

memory Any device capable of storing information. This term is usually used to indicate volatile random access memory (RAM) capable of high-speed access to any portion of the memory space, but incapable of storing information without power.

Memory Diagnostics Tool A diagnostic utility in Windows Vista that is used to test your computer's memory.

MHz See megahertz.

Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) A remote access authentication protocol that adds to the services provided by CHAP by providing mutual authentication, different encryption keys for sending and receiving, and stronger data encryption keys. Windows 2000 (all versions), Windows XP (all versions), Windows Server 2003, and Windows Vista can use MS-CHAPv2 with dial-up and virtual private network (VPN) connections. If you are using Windows NT 4 (all versions) or Windows 95/98 computers, you can use MS-CHAPv2 authentication only with VPN connections.

Microsoft Management Console (MMC) A console framework for management applications. The MMC provides a common environment for snap-ins.

Microsoft Point-to-Point Encryption (MPPE) A remote data encryption standard that is a Point-to-Point Protocol (PPP) data encryption option that uses Rivest-Shamir-Adleman (RSA) RC4 encryption. MPPE supports strong (128-bit key) or standard (40-bit key) encryption. To use MPPE data encryption over a dial-up or virtual private network (VPN) connection, the remote client and server that will be accessed must use the MS-CHAPv2 or EAP authentication protocols.

Microsoft Spynet An online community that can help you know how others respond to software that has not yet been classified by Microsoft.

MMC See Microsoft Management Console.

modem Modulator/demodulator. A device used to create an analog signal suitable for transmission over telephone lines from a digital data stream. Modern modems also include a command set for negotiating connections and data rates with remote modems and for setting their default behavior.

MPPE See Microsoft Point-to-Point Encryption.

MS-CHAPv2 See Microsoft Challenge Handshake Authentication Protocol Version 2.

multibooting The process of allowing a computer to boot multiple operating systems.

N

Narrator A utility used to read aloud on-screen text, dialog boxes, menus, and buttons. This utility requires some type of sound output device.

Nbtstat Command-line utility that is used to display TCP/IP connection protocol statistics over NetBIOS over TCP/IP.

NetBEUI See NetBIOS Extended User Interface.

NetBIOS See Network Basic Input/Output System.

NetBIOS Extended User Interface (NetBEUI) A simple Network layer transport protocol developed to support NetBIOS installations. NetBEUI is not routable, and so it is not appropriate for larger networks.

NetWare A popular network operating system developed by Novell in the early 1980s. NetWare is a cooperative, multitasking, highly optimized, dedicated-server network operating system that has client support for most major operating systems. Recent versions of NetWare include graphical client tools for management from client stations. At one time, NetWare accounted for more than 70 percent of the network operating system market.

network adapter The hardware used to connect computers (or other devices) to the network.

Network and Sharing Center The new networking hub in Windows Vista that you can use to view and configure your network devices, as well as share files and printers on your network.

Network Basic Input/Output System (NetBIOS) A client/server interprocess communications (IPC) service developed by IBM in the early 1980s. NetBIOS presents a relatively primitive mechanism for communication in client/server applications, but its widespread acceptance and availability across most operating systems make it a logical choice for simple network applications.

Network Configuration Operators group Members of the Network Configuration Operators group have some administrative rights to manage the computer's network configuration.

Network group A special group that includes the users who access a computer's resources over a network connection.

Network Places The folder that provides access to shared resources, such as local network resources and web resources.

network printer A printer that is available to local and network users. A network printer can use a physical port or a logical port.

New Technology File System (NTFS) A secure, transaction-oriented file system developed for Windows NT and used by Windows 2000, Windows XP, and Windows Server 2003. NTFS offers features such as local security on files and folders, data compression, disk quotas, and data encryption.

NTFS See New Technology File System.

NTFS permissions Permissions used to control access to NTFS folders and files. Access is configured by allowing or denying NTFS permissions to users and groups.

O

offline files and folders A Windows Vista feature that allows network folders and files to be stored on Windows Vista clients. Users can access network files even if the network location is not available.

On-Screen Keyboard A utility that displays a keyboard on the screen and allows users to enter keyboard input by using a mouse or other input device.

optimization Any effort to reduce the workload on a hardware component by eliminating, obviating, or reducing the amount of work required of the hardware component through any means. For instance, file caching is an optimization that reduces the workload of a hard disk drive by reducing the number of requests sent to the hard disk drive.

organizational unit (OU) In Active Directory, an organizational unit is a generic folder used to create a collection of objects. An OU can represent a department, division, location, or project group. Used to ease administration of AD objects and as a unit to which group policy can be deployed.

OU See organizational unit.

outbound rule A Windows Firewall rule that applies to network traffic sent from the computer.

owner The user associated with an NTFS file or folder who is able to control access and grant permissions to other users.

P

pagefile Logical memory that exists on the hard drive. If a system is experiencing excessive paging (swapping between the pagefile and physical RAM), it needs more memory.

PAP See Password Authentication Protocol.

Parental Controls A security feature of Windows Vista that allows you to control and monitor the websites that your children visit.

partition A section of a hard disk that can contain an independent file system volume. Partitions can be used to keep multiple operating systems and file systems on the same hard disk.

Password Authentication Protocol (PAP) A remote access authentication protocol. It is the simplest authentication method. It uses unencrypted, plain-text passwords. You would use PAP if the server you were connecting to didn't support secure validations or you were troubleshooting remote access and wanted to use the most basic authentication option.

password policies Windows Vista policies used to enforce security requirements on the computer. Password policies are set on a per-computer basis, and they cannot be configured for specific users. Password policies are set through account policies.

PB See petabyte.

PC Card A special credit card–sized device used to add devices to a laptop computer. Also called a Personal Computer Memory Card International Association (PCMCIA) card.

PCI See Peripheral Component Interconnect.

PCMCIA card See Personal Computer Memory Card International Association (PCMCIA) card.

People Near Me A peer-to-peer networking component of Windows Vista that enables you to discover and connect to other people on the local subnet. This feature can be used to enable multiple users to easily collaborate on a project using applications such as Windows Meeting Space.

Peripheral Component Interconnect (PCI) A high-speed, 32/64-bit bus interface developed by Intel and widely accepted as the successor to the 16-bit Industry Standard Architecture (ISA) interface. PCI devices support input/output (I/O) throughput about 40 times faster than the ISA bus.

Performance Information and Tools An application in Windows Vista that provides you with a numerical score that lets you know how well each of your computer's subsystems performs.

permissions Security constructs used to regulate access to resources by username or group affiliation. Permissions can be assigned by administrators to allow any level of access, such as read-only, read/write, or delete, by controlling the ability of users to initiate object services. Security is implemented by checking the user's security identifier (SID) against each object's discretionary access control list (DACL).

Personal Computer Memory Card International Association (PCMCIA) card A special credit card–sized device used to add devices to a laptop computer. Also called a PC Card.

petabyte A computer storage measurement that is equal to 1,024 terabytes.

phishing A method used to attempt to trick someone into providing personal and financial information by claiming to be a legitimate company requesting information.

Phishing Filter A feature of Windows Vista that provides protection and phishing attacks by checking websites to determine whether they are known to be fraudulent or contain characteristics common to fraudulent sites.

ping A command used to send an Internet Control Message Protocol (ICMP) echo request and echo reply to verify that a remote computer is available.

plain text Data or text that has not been encrypted. Also called clear text.

Plug and Play A technology that uses a combination of hardware and software to allow the operating system to automatically recognize and configure new hardware without any user intervention.

Point-to-Point Protocol (PPP) A set of remote authentication protocols used by Windows during remote access for interoperability with third-party remote access software.

Point-to-Point Tunneling Protocol An open industry-standard developed by Microsoft and other industry leaders to provide support for tunneling of Point-to-Point Protocol (PPP) frames through an Internet Protocol (IP) network. PPP provides authentication, compression, and encryption services.

policies General controls that enhance the security of an operating environment. In Windows Vista, policies affect restrictions on password use and rights assignments and determine which events will be recorded in the Security log.

POP3 See Post Office Protocol 3.

Pop-up Blocker A feature of Internet Explorer that prevents pop-ups from being displayed by web pages.

POST See Power-On Self-Test.

Post Office Protocol 3 (POP3) A protocol used to receive e-mail messages over the Internet.

power plans Preconfigured options for power management in Windows Vista.

Power-On Self-Test (POST) A part of the boot sequence. The POST detects the computer's processor, how much memory is present, what hardware is recognized, and whether the BIOS is standard or has Plug and Play capabilities.

Power Saver power plan A power plan included with Windows Vista that is optimized for power savings rather than performance.

Power Users group A built-in group that is included for backward compatibility purposes.

PPP See Point-to-Point Protocol.

PPTP See Point-to-Point Tunneling Protocol.

Preboot Execution Environment (PXE) A technology that allows a client computer to remotely boot and connect to a Windows Deployment Services (WDS) server.

previous versions A feature of Windows Vista for creating shadow copies of files so that the files can be restored to a previous state. If System Restore is not enabled, the shadow copies cannot be created.

primary partition A part of basic storage on a disk. The primary partition is the first partition created on a hard drive. The primary partition uses all of the space that is allocated to the partition. This partition is usually marked as active and is the partition that is used to boot the computer.

print device The actual physical printer or hardware device that generates printed output.

printer In Windows Vista terminology, the software interface between the physical printer (see print device) and the operating system.

priority A level of execution importance assigned to a thread. In combination with other factors, the priority level determines how often that thread will get computer time according to a scheduling algorithm.

privilege escalation Method by which UAC protects computers by requiring authentication when performing a task that requires administrative privileges.

Problem Reports and Solutions A new application in Windows Vista that enables you to track system problems and allow you to check for potential solutions to those problems. Problem Reports and Solutions replaces Dr. Watson.

process A running program containing one or more threads. A process encapsulates the protected memory and environment for its threads.

processor A circuit designed to automatically perform lists of logical and arithmetic operations. Unlike microprocessors, processors may be designed from discrete components rather than be a monolithic integrated circuit.

processor affinity The association of a processor with specific processes that are running on the computer. Processor affinity is used to configure multiple processors.

Program Compatibility Wizard A utility that helps you run legacy applications under Windows Vista.

Protected Mode A security feature of Internet Explorer that prevents malicious code from being run outside of the Temporary Internet Files directory, unless specifically granted access.

protocol An established rule of communication adhered to by the parties operating under it. Protocols provide a context in which to interpret communicated information. Computer protocols are rules used by communicating devices and software services to format data in a way that all participants understand.

PSTN See Public Switched Telephone Network.

Public Switched Telephone Network (PSTN) The network that provides regular, analog phone service.

PXE See Preboot Execution Environment.

Q

Quarantined Items Location in Windows Defender where suspicious software applications are kept until you remove them.

R

RAM See random access memory.

random access memory (RAM) Integrated circuits that store digital bits in massive arrays of logical gates or capacitors. RAM is the primary memory store for modern computers, storing all running software processes and contextual data.

RAS See Remote Access Service.

ReadyBoost A new technology included with Windows Vista that allows you to use USB flash memory to increase the performance of a computer by storing data on the flash memory rather than on the hard disk's pagefile. Windows is able to access data stored on flash drives more quickly than data stored on hard drives.

ReadyDrive ReadyDrive is a new technology included with Windows Vista that can be used to speed up the boot process, resume from a hibernation state faster, and conserve battery power. ReadyDrive relies on new hybrid hard disks, which uses flash memory technology in conjunction with mechanical hard disk technology.

Really Simple Syndication (RSS) RSS is a content syndication technology that enables a website to syndicate content via an RSS file, which is a formatted XML document.

Recycle Bin A folder that holds files and folders that have been deleted. Files can be retrieved or cleared (for permanent deletion) from the Recycle Bin.

reference computer The Windows Vista disk image used as the source for automated installations.

REGEDIT A Windows program, the Registry Editor, which is used to edit the Registry.

Registry A database of settings required and maintained by Windows Vista and its components. The Registry contains all of the configuration information used by the computer. It is stored as a hierarchical structure and is made up of keys, hives, and value entries.

Registry Editor The utility used to edit the Windows Vista Registry. You can use REGEDIT or REGEDT32.

Reliability and Performance Monitor An application in Windows Vista that is used to measure the performance and reliability of a local or remote computer on the network. Reliability and Performance Monitor replaces Performance Logs and Alerts (PLA), Server Performance Advisor (SPA), and System Monitor.

remote access connections A method for allowing remote clients connectivity to a private network or the Internet.

Remote Access Service (RAS) A service that allows network connections to be established over a modem connection, an Integrated Services Digital Network (ISDN) connection, or a null-modem cable. The computer initiating the connection is called the RAS client; the answering computer is called the RAS server.

Remote Assistance A mechanism for requesting help for *x*86-based computers through Windows Messenger and e-mail or by sending a file requesting help. To use Remote Assistance, the computer requesting help and the computer providing help must be using Windows Vista, Windows XP Professional, or Windows Server 2003 and must have some sort of interconnectivity.

Remote Desktop A utility that allows you to take control of a remote computer's keyboard, video, and mouse. This tool does not require that someone collaborate with you on the remote computer. While the remote computer is being accessed, it remains locked and any actions that are performed remotely will not be visible to the monitor that is attached to the remote computer.

Remote Desktop Users group A special group automatically created on Windows Vista computers that is used in conjunction with the Remote Desktop service.

Remote Desktop Web Connection A Windows Vista utility that enables you to connect to a remote computer over the Internet. Before you can connect, Remote Desktop Web Connection must be installed on the remote computer.

remote installation Installation of Windows Vista performed remotely through Windows Deployment Services (WDS).

Remote Installation Services (RIS) A technology used in previous versions of Windows that allows the remote installation of those versions of Windows, such as Windows XP Professional. A RIS server installs Windows XP Professional on RIS clients. This technology has been updated in Windows Vista and is now called Windows Deployment Services.

Replicator group A built-in group that supports directory replication, which is a feature used by domain servers. Only domain user accounts that will be used to start the replication service should be assigned to this group.

resource Any useful service, such as a shared folder or a printer.

restore point Recovery point created by System Protection and used by System Restore to restore the system files and settings on your computer to an earlier point in time.

resolution The number of pixels viewable on a computer monitor.

RIS See Remote Installation Services.

roaming profile A user profile that is stored and configured to be downloaded from a server. Roaming profiles allow users to access their profiles from any location on the network.

router A Network layer device that moves packets between networks. Routers provide internetwork connectivity.

RSS See Really Simple Syndication.

S

Safe Mode A Windows Vista Advanced Boot Options menu item that loads the absolute minimum of services and drivers that are needed to start Windows Vista. The drivers that are loaded with Safe Mode include basic files and drivers for the mouse, monitor, keyboard, hard drive, standard video driver, and default system services. Safe Mode is considered a diagnostic mode. It does not include networking capabilities.

Safe Mode with Command Prompt A Windows Vista Advanced Boot Options menu item that starts Windows Vista in Safe Mode, but after you log into Windows Vista, only a command prompt is displayed. This mode does not provide access to the Desktop.

Safe Mode with Networking A Windows Vista Advanced Boot Options menu item that starts Windows Vista in Safe Mode but adds networking features.

SCSI See Small Computer Systems Interface.

search providers The website used when entering search phrases into the Instant Search box. Multiple search providers can be installed, and custom providers can be created.

security The measures taken to secure a system against accidental or intentional loss, usually in the form of accountability procedures and use restriction—for example, through NTFS permissions and share permissions.

security identifier (SID) A unique code that identifies a specific user or group to the Windows Vista security system. SIDs contain a complete set of permissions for that user or group.

Security log A log that tracks events that are related to Windows Vista auditing. The Security log can be viewed through the Event Viewer utility.

security option policies Policies used to configure security for the computer. Security option policies apply to computers rather than to users or groups. These policies are set through the Local Computer Policy snap-in.

service A process dedicated to implementing a specific function for another process. Many Windows Vista components are services used by user-level applications.

Service group A special group that includes users who log on as a user account that is used only to run a service.

service pack An update to the Windows Vista operating system that includes bug fixes and enhancements.

service set identifier (SSID) An identifier used by wireless devices to identify a wireless network.

Services utility A Windows Vista utility used to manage the services installed on the computer.

SETUPSNK.EXE File that launches the Wireless Network Setup Wizard to automatically configure a computer with wireless network settings.

shadow copy A copy of a file created in the background in order to allow the file to be restored to a previous state.

share A resource such as a folder or printer shared over a network.

share permissions Permissions used to control access to shared folders. Share permissions can be applied only to folders, as opposed to NTFS permissions, which are more complex and can be applied to folders and files.

shared folder A folder on a Windows Vista computer that network users can access.

Shared Folders A Windows Vista utility for managing shared folders on the computer.

sharing The process of allowing network users to access a folder located on a computer.

shortcut A quick link to an item that is accessible from a computer or network, such as a file, program, folder, printer, or computer. Shortcuts can exist in various locations including the Desktop and the Start Menu or within folders.

SID See security identifier.

Simple Mail Transfer Protocol (SMTP) An Internet protocol for transferring mail between Internet hosts. SMTP is often used to upload mail directly from the client to an intermediate host but can only be used to receive mail by computers constantly connected to the Internet.

simple volume A dynamic disk volume that contains space from a single disk. The space from the single disk can be contiguous or noncontiguous. Simple volumes are used when the computer has enough disk space on a single drive to hold an entire volume.

sleep A new power management option included with Windows Vista. Sleep mode combines the features of hibernate and standby. When a computer enters the sleep power state, data including window locations and running applications is saved to the hard disk, and that session is available within seconds when the computer wakes.

Small Computer Systems Interface (SCSI) A high-speed, parallel-bus interface that connects hard disk drives, CD-ROM drives, tape drives, and many other peripherals to a computer. SCSI is the mass-storage connection standard among all computers except IBM compatibles, which use SCSI or IDE.

smart card A special piece of hardware with a microchip, used to store public and private keys, passwords, and other personal information securely. Can be used for other purposes, such as telephone calling and electronic cash payments.

SMTP See Simple Mail Transfer Protocol.

snap-in An administrative tool developed by Microsoft or a third-party vendor that can be added to the Microsoft Management Console (MMC) in Windows Vista.

spanned volume A dynamic disk volume that consists of disk space on 2 to 32 dynamic drives. Spanned volume sets are used to dynamically increase the size of a dynamic volume. With spanned volumes, the data is written sequentially, filling space on one physical drive before writing to space on the next physical drive in the spanned volume set.

special group A group used by Windows Vista, in which membership is automatic if certain criteria are met. Administrators cannot manage special groups.

SSID See service set identifier

Standard User Account A type of user account type that can perform most day-to-day tasks, but does not have administrative capabilities. Running as a Standard User increases security by limiting the possibility of a virus or other malicious code from infecting the computer and making systemwide changes, as Standard User accounts are unable to make systemwide changes.

standby A power management option. Standby does not save data automatically as hibernation does. With standby you can access your computer more quickly than a computer that

is in hibernation, usually through a mouse click or keystroke, and the Desktop appears as it was prior to the standby. The response time depends on the level of your computer's standby state. On an Advanced Configuration and Power Interface (ACPI)–compliant computer, there are three levels of standby, each level putting the computer into a deeper sleep. The first level turns off power to the monitor and hard drives. The second level turns off power to the CPU and cache. The third level supplies power to RAM only and preserves the Desktop in memory.

Start Menu A Windows Vista Desktop item, located on the taskbar. The Start Menu contains a list of options and programs that can be run.

Start Windows Normally A Windows Vista Advanced Boot Option menu item that allows Windows to start normally.

Startup Repair Tool A Windows Vista utility that is used to repair missing or corrupted system files without affecting personal files.

stripe set A single volume created across multiple hard disk drives and accessed in parallel for the purpose of optimizing disk-access time. NTFS can create stripe sets.

striped volume A dynamic disk volume that stores data in equal stripes between 2 to 32 dynamic drives. Typically, administrators use striped volumes when they want to combine the space of several physical drives into a single logical volume and increase disk performance.

subnet mask A number mathematically applied to IP addresses to determine which IP addresses are a part of the same subnetwork as the computer applying the subnet mask.

Success Audit event An Event Viewer entry that indicates the occurrence of an event that has been audited for success, such as a successful logon.

super mandatory profile A type of mandatory user profile with an additional layer of security that does not enable a user to log on if that user's mandatory profile is not available.

Sysprep See System Preparation Tool.

System Configuration A Windows Vista utility that is used to help you view and troubleshoot how Windows Vista starts and what programs and services launch at startup.

System group A Windows Vista special group that contains system processes that access specific functions as a user.

System Information A Windows Vista utility used to collect and display information about the computer's current configuration.

System log A log that tracks events that relate to the Windows Vista operating system. The System log can be viewed through the Event Viewer utility.

system partition The active partition on an *x*86–based computer that contains the hardware-specific files used to load the Windows Vista operating system.

System Preparation Tool (Sysprep) A Windows Vista utility used to prepare a disk image for disk duplication.

System Restore A Windows Vista utility used to monitor a computer for changes and creates restore points that can be used to restore the system files and settings on your computer to an earlier point in time without affecting your personal files.

System Tool A Windows Vista tool found in Control Panel that is used to manage performance options for your computer.

System Tools A Computer Management utility grouping that provides access to utilities for managing common system functions. The System Tools utility includes the Event Viewer, System Information, Performance Logs and Alerts, Shared Folders, Device Manager, and Local Users and Groups utilities.

T

Tablet PC Input Panel A feature included with Tablet PCs that enables text to be inputted using a stylus instead of typing on a keyboard.

Task Manager A Windows Vista utility that can be used to start, end, or prioritize applications. The Task Manager shows the applications and processes that are currently running on the computer, as well as CPU and memory usage information.

Task Scheduler A Windows Vista utility used to schedule tasks to occur at specified intervals or when certain events occur.

taskbar A Windows Vista Desktop item, which appears across the bottom of the screen by default. The taskbar contains the Start Menu and buttons for any programs, documents, or windows that are currently running on the computer. Users can switch between open items by clicking the item in the taskbar.

TB See terabyte.

TCP See Transmission Control Protocol.

TCP/IP See Transmission Control Protocol/Internet Protocol.

terabyte (TB) A computer storage measurement that equals 1,024 gigabytes.

Terminal Server User group A Windows Vista special group that includes users who log on through Terminal Services.

TFTP See Trivial File Transfer Protocol.

thread A list of instructions running in a computer to perform a certain task. Each thread runs in the context of a process, which embodies the protected memory space and the environment of the threads. Multithreaded processes can perform more than one task at the same time.

Token Ring A LAN technology that was developed by IBM in the 1970s and is defined by the IEEE 802.5 specification. In a Token Ring network, all nodes are wired into a physical

ring. A token is used to manage communications. Token Ring is more difficult to install and configure and is more expensive than Ethernet. It is rarely used in corporate or home environments. Token Ring is most typically used in networks that use IBM equipment and require IBM connectivity.

TPM See Trusted Platform Module

Transmission Control Protocol (TCP) A Transport layer protocol that implements guaranteed packet delivery using the IP protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP) A suite of Internet protocols upon which the global Internet is based. TCP/IP is a general term that can refer either to the TCP and IP protocols used together or to the complete set of Internet protocols. TCP/IP is the default protocol for Windows Vista.

Trivial File Transfer Protocol (TFTP) A network application that is simpler than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP is used to download Windows Vista components from the Windows Deployment Services (RIS) server to the WDS clients. TFTP uses the User Datagram Protocol (UDP).

Trusted Platform Module (TPM) A chip that contains the BitLocker security key. It also monitors the computer for potential security risks, such as disk errors or changes made to BIOS, hardware, system files, or startup components

U

UAC See User Account Control.

UFD See Universal Flash Device.

Unattend.xml An answer file used in conjunction with unattended installations to provide answers to installation queries that would normally be supplied by an interactive user.

unattended installation A method of installing Windows Vista remotely with little or no user intervention. Unattended installation uses a distribution server or the Windows Vista installation media to install Windows Vista on a target computer.

UNC See Universal Naming Convention.

Uniform Resource Locator (URL) An Internet standard naming convention for identifying resources available via various TCP/IP application protocols. For example, `http://www.microsoft.com` is the URL for Microsoft's World Wide Web server site. A URL allows easy hypertext references to a particular resource from within a document or mail message. A URL always has the domain name on the right and the host name on the left.

Universal Flash Device (UFD) A bootable USB device such as a USB memory key or an external USB hard drive.

Universal Naming Convention (UNC) A multivendor, multiplatform convention for identifying shared resources on a network. UNC names follow the naming convention \\computername\sharename.

Universal Serial Bus (USB) An external bus standard that allows USB devices to be connected through a USB port. USB supports transfer rates up to 12Mbps. A single USB port can support up to 127 devices.

upgrade A method for installing Windows Vista that preserves existing settings and preferences when converting to the newer operating system from a previous version of Windows.

URL See Uniform Resource Locator.

USB See Universal Serial Bus.

User Account Control (UAC) A security feature of Windows Vista that requires users to acknowledge and confirm that they want to perform a task that requires administrative privileges. This helps prevent malicious code from being run without the user's knowledge.

user profile A profile that stores a user's Desktop configuration and other preferences. A user profile can contain a user's Desktop arrangement, program items, personal program groups, network and printer connections, screen colors, mouse settings, and other personal preferences. Administrators can create mandatory profiles, which cannot be changed by the users, and roaming profiles, which users can access from any computer they log on to.

user right policies Policies that control the rights that users and groups have to accomplish network tasks. User right policies are set through the Local Computer Policy snap-in.

User State Migration Tool (USMT) A utility used by administrators to migrate users from one computer to another via a command-line utility.

username A user's account name in a logon authenticated system.

Users group A Windows Vista built-in group that includes end users who should have very limited system access. After a clean install of Windows Vista, the default settings for this group prohibit users from compromising the operating system or program files. By default, all users who have been created on the computer, except the Guest account, are members of the Users group.

USMT See User State Migration Tool.

V

Verbose event An Event Viewer event type that is used for the least severe events.

video adapter The hardware device that outputs the display to the monitor.

virtual memory A kernel service that stores memory pages not currently in use on a mass-storage device to free the memory occupied for other uses. Virtual memory hides the memory-swapping process from applications and higher-level services.

virtual private network (VPN) A private network that uses secure links across private or public networks (such as the Internet). When data is sent over the remote link, it is encapsulated, encrypted, and requires authentication services.

volume A storage area on a Windows Vista dynamic disk. Dynamic volumes cannot contain partitions or logical drives. Windows Vista dynamic storage supports three dynamic volume types: simple volumes, spanned volumes, and striped volumes. Dynamic volumes are accessible only to Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. They are not accessible through DOS, Windows 9*x*, Windows Me, or Windows NT.

VPN See virtual private network.

W

WAIK See Windows Automated Installation Kit.

WAN See wide area network.

Warning event An Event Viewer entry that indicates that you should be concerned with the event. The event may not be critical in nature, but it is significant and may be indicative of future errors.

WDS See Windows Deployment Services.

WDS Service A service that manages the Windows Deployment Services (WDS) process.

WDSUTIL A command-line utility for configuring WDS in your environment.

web browser An application that makes HTTP requests and formats the resultant HTML documents for the users. Most web browsers understand all standard Internet protocols.

Welcome Center A Windows Vista application that launches at startup and contains links to help you get started using Windows Vista. It also contains links that direct you to offers from Microsoft.

WEP See Wired Equivalent Privacy.

WFAS See Windows Firewall with Advanced Security.

Wi-Fi Protected Access (WPA) A method of wireless encryption.

wide area network (WAN) Used to connect two geographically dispersed areas together via a persistent connection. Connection methods used with WANs include T1 carried leased line, cable modem, DSL, and Frame Relay.

Win32 The set of application services provided by the 32-bit versions of Microsoft Windows: Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

Windows 9*x* The 32-bit Windows 95, Windows 98, and Windows Me versions of Microsoft Windows for medium-range, *x*86-based personal computers. This system includes peer networking services, Internet support, and strong support for older DOS applications and peripherals.

Windows Activation Method by which Microsoft activates Windows Vista on a computer in an effort to reduce software piracy.

Windows Aero A new user interface theme installed with Windows Vista that displays Windows with glass-like transparency.

Windows Anytime Upgrade A feature of Windows Vista that enables you to upgrade Vista Home Basic, Home Premium, or Business to a more advanced edition of Windows Vista.

Windows Automated Installation Kit (WAIK) A suite of tools that provides utilities that can be used for automating the installation of Windows Vista.

Windows Calendar A new application included with Windows Vista that is used to store appointments and tasks. Windows Calendar integrates with Windows Mail.

Windows CardSpace A new application included with Windows Vista that enables you to create cards that can be used to send personal information to websites.

Windows Complete PC Backup A Windows Vista utility that enables you to create images of your entire computer.

Windows Complete PC Restore A Windows Vista utility that enables you to restore images of your entire computer.

Windows Contacts A new application included with Windows Vista that is used to store contact information for individuals. Windows Contacts integrates with Windows Mail.

Windows Defender A Windows Vista utility that offers real-time protection from spyware and other unwanted software.

Windows Deployment Services (WDS) An updated version of Remote Installation Services. A suite of components that allow you to remotely install Windows Vista on client computers.

Windows Easy Transfer A utility used by administrators to migrate files and settings from one computer to another computer. This option is used when you purchase a new computer with Windows Vista already installed, and you want to migrate files and settings from an existing computer that is running a previous version of Windows.

Windows Experience Index A base score, provided by Performance Information and Tools, that indicates how well your computer should run applications.

Windows Fax and Scan A Windows Vista utility for configuring and managing fax machines and scanners.

Windows Firewall Utility in Windows Vista that helps to prevent unauthorized users or malicious software from accessing your computer. Windows Firewall does not allow unsolicited traffic to pass through the firewall.

Windows Firewall with Advanced Security (WFAS) Utility in Windows Vista that enables you to configure advanced firewall options.

Windows Internet Name Service (WINS) A network service for Microsoft networks that provides Windows computers with the IP address for specified NetBIOS computer names, facilitating browsing and intercommunication over TCP/IP networks.

Windows Mail E-mail application included with Windows Vista. This application replaces Outlook Express.

Windows Media Center A multimedia application included with Windows Vista that enables you to record and watch TV, play audio or video, watch a slide show, listen to the radio, burn a CD or DVD, stream or download online music, and play online games on demand.

Windows Media Player 11 A multimedia application included with Windows Vista that enables you to play digital media, organize your media files, rip music from CDs, burn CDs and DVDs, synchronize files to a portable music player, and shop for digital media online.

Windows Meeting Space Windows Vista's replacement for NetMeeting that allows you to collaborate with other users, share an application, show your Desktop, and create notes for other users.

Windows NT The predecessor to Windows 2000 that is a 32-bit version of Microsoft Windows for powerful Intel, Alpha, PowerPC, or MIPS-based computers. These operating systems include Windows NT 3.1, Windows NT 3.5, Windows NT 3.51, and Windows NT 4 and include peer networking services, server networking services, Internet client and server services, and a broad range of utilities.

Windows Preinstallation Environment An environment similar to MS-DOS, but based on the Windows kernel. It provides the minimal set of features required to run Windows Setup and to access disk images over the network.

Windows Security Center A Windows Vista utility that allows you to monitor and configure critical settings through a centralized dialog box. Critical settings include Firewall, Automatic Updating, Malware Protection, and Other Security Settings.

Windows Sidebar A feature of Windows Vista that stores gadgets that can provide quick access to information on the desktop.

Windows SideShow An application included with Windows Vista that enables you to view information from your computer by using an alternative display device. These devices can be integrated into your computer, such as a small LCD display on the lid of a laptop or a keyboard, or they can be separate from your computer, such as a mobile phone or a Windows SideShow-enabled TV or LCD.

Windows Sync Center An application included with Windows Vista that is used to synchronize music and files between your computer and a network folder or mobile device.

Windows System Image Manager A Windows Vista utility used to create answer files for unattended installations.

Windows Update A utility that connects the computer to Microsoft's website and checks the files to make sure that they are the most up-to-date versions.

Windows Vista The current version of the Windows operating system for desktop environments. Windows Vista provides many security and usability enhancements over previous versions of Windows.

Windows Vista Business A business version of the Windows Vista operating system.

Windows Vista Enterprise A business version of the Windows Vista operating system that includes the features found in Windows Vista Business plus BitLocker Drive Encryption and Virtual PC Express. Vista Enterprise is only available via Microsoft Software Assurance or a Microsoft Enterprise Agreement

Windows Vista Home Basic A consumer version of the Windows Vista operating system that is recommended for basic computer needs, such as accessing the Internet, checking e-mail, and basic document creation.

Windows Vista Home Premium A consumer version of the Windows Vista operating system that includes the features in Windows Vista Home Basic plus digital entertainment features.

Windows Vista Starter A limited version of the Windows Vista operating system that is only available in emerging markets; it is not available in the United States or Europe.

Windows Vista Ultimate The most advanced version of the Windows Vista operating system. Vista Ultimate contains everything that Windows Vista has to offer.

Windows Vista Upgrade Advisor A utility in Windows Vista that can check the compatibility of your system, devices, and installed applications before or during Vista installation and then provide the results to you.

Windows XP Professional The previous version of the Windows operating system for desktop environments. Windows XP Professional integrated the best features of Windows 98, Windows Me, and Windows 2000 Professional; supported a wide range of hardware; made the operating system easier to use; and reduced the cost of ownership.

WINS See Windows Internet Name Service.

WINS server The server that runs WINS and is used to resolve NetBIOS computer names to IP addresses.

Wired Equivalent Privacy (WEP) A form of encryption for wireless networks that is relatively easy for hackers to decrypt due to a weak initialization vector.

workgroup In Microsoft networks, a collection of related computers, such as those used in a department, that do not require the uniform security and coordination of a domain. Workgroups are characterized by decentralized management, as opposed to the centralized management that domains use.

WPA See Wi-Fi Protected Access.

WPA2 A more advanced form of WPA encryption.

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

MCTS: Microsoft Windows Vista Client Configuration Study Guide

Exam 70-620: TS: Microsoft Windows Vista, Configuring

OBJECTIVE	CHAPTER
INSTALLING AND UPGRADING WINDOWS VISTA	
Identify hardware requirements.	1
Perform a clean installation.	1
Upgrade to Windows Vista from previous versions of Windows.	1
Upgrade from one edition of Windows Vista to another edition.	1
Troubleshoot Windows Vista installation issues.	1
Install and configure Windows Vista drivers.	1
CONFIGURING AND TROUBLESHOOTING POST-INSTALLATION SYSTEM SETTINGS	
Troubleshoot post-installation configuration issues.	3, 4, 5, 7
Configure and troubleshoot Windows Aero.	3, 4
Configure and troubleshoot parental controls.	9
Configure Windows Internet Explorer.	9
CONFIGURING WINDOWS SECURITY FEATURES	
Configure and troubleshoot User Account Control.	5, 6
Configure Windows Defender.	6
Configure Dynamic Security for Internet Explorer 7.	9
Configure security settings in Windows Firewall.	6
CONFIGURING NETWORK CONNECTIVITY	
Configuring networking by using the Network and Sharing Center.	8
Troubleshoot connectivity issues.	8
Configure Remote Access.	8

Sybex®
An Imprint of
WILEY

OBJECTIVE	CHAPTER
CONFIGURING APPLICATIONS INCLUDED WITH WINDOWS VISTA	
Configure and troubleshoot media applications.	10
Configure Windows Mail.	10
Configure Windows Meeting Space.	10
Configure Windows Calendar.	10
Configure Windows Fax and Scan.	10
Configure Windows Sidebar.	4, 10
MAINTAINING AND OPTIMIZING SYSTEMS THAT RUN WINDOWS VISTA	
Troubleshoot performance issues.	11
Troubleshoot reliability issues by using built-in diagnostic tools.	3, 7, 11
Configure Windows Update.	1
Configure Data Protection.	7, 11
CONFIGURING AND TROUBLESHOOTING MOBILE COMPUTING	
Configure Mobile Display Settings.	3
Configure Mobile Devices.	3
Configure Tablet PC software.	3
Configure Power Options.	3

Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit Microsoft's website (`www.microsoft.com/learning`) for the most current listing of exam objectives.

Wiley Publishing, Inc.
End-User License Agreement

READ THIS. You should carefully read these terms and conditions before opening the software packet(s) included with this book "Book". This is a license agreement "Agreement" between you and Wiley Publishing, Inc. "WPI". By opening the accompanying software packet(s), you acknowledge that you have read and accept the following terms and conditions. If you do not agree and do not want to be bound by such terms and conditions, promptly return the Book and the unopened software packet(s) to the place you obtained them for a full refund.

1. License Grant. WPI grants to you (either an individual or entity) a nonexclusive license to use one copy of the enclosed software program(s) (collectively, the "Software," solely for your own personal or business purposes on a single computer (whether a standard computer or a workstation component of a multi-user network). The Software is in use on a computer when it is loaded into temporary memory (RAM) or installed into permanent memory (hard disk, CD-ROM, or other storage device). WPI reserves all rights not expressly granted herein.

2. Ownership. WPI is the owner of all right, title, and interest, including copyright, in and to the compilation of the Software recorded on the physical packet included with this Book "Software Media". Copyright to the individual programs recorded on the Software Media is owned by the author or other authorized copyright owner of each program. Ownership of the Software and all proprietary rights relating thereto remain with WPI and its licensers.

3. Restrictions On Use and Transfer.

(**a**) You may only (i) make one copy of the Software for backup or archival purposes, or (ii) transfer the Software to a single hard disk, provided that you keep the original for backup or archival purposes. You may not (i) rent or lease the Software, (ii) copy or reproduce the Software through a LAN or other network system or through any computer subscriber system or bulletin-board system, or (iii) modify, adapt, or create derivative works based on the Software.

(**b**) You may not reverse engineer, decompile, or disassemble the Software. You may transfer the Software and user documentation on a permanent basis, provided that the transferee agrees to accept the terms and conditions of this Agreement and you retain no copies. If the Software is an update or has been updated, any transfer must include the most recent update and all prior versions.

4. Restrictions on Use of Individual Programs. You must follow the individual requirements and restrictions detailed for each individual program in the About the CD-ROM appendix of this Book or on the Software Media. These limitations are also contained in the individual license agreements recorded on the Software Media. These limitations may include a requirement that after using the program for a specified period of time, the user must pay a registration fee or discontinue use. By opening the Software packet(s), you will be agreeing to abide by the licenses and restrictions for these individual programs that are detailed in the About the CD-ROM appendix and/or on the Software Media. None of the material on this Software Media or listed in this Book may ever be redistributed, in original or modified form, for commercial purposes.

5. Limited Warranty.

(**a**) WPI warrants that the Software and Software Media are free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of purchase of this Book. If WPI receives notification within the warranty period of defects in materials or workmanship, WPI will replace the defective Software Media.

(**b**) WPI AND THE AUTHOR(S) OF THE BOOK DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE PROGRAMS, THE SOURCE CODE CONTAINED THEREIN, AND/OR THE TECHNIQUES DESCRIBED IN THIS BOOK. WPI DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE.

(**c**) This limited warranty gives you specific legal rights, and you may have other rights that vary from jurisdiction to jurisdiction.

6. Remedies.

(**a**) WPI's entire liability and your exclusive remedy for defects in materials and workmanship shall be limited to replacement of the Software Media, which may be returned to WPI with a copy of your receipt at the following address: Software Media Fulfillment Department, Attn.: *MCTS: Microsoft Windows Vista Client Configuration Study Guide (70-620)*, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, or call 1-800-762-2974. Please allow four to six weeks for delivery. This Limited Warranty is void if failure of the Software Media has resulted from accident, abuse, or misapplication. Any replacement Software Media will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

(**b**) In no event shall WPI or the author be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the Book or the Software, even if WPI has been advised of the possibility of such damages.

(**c**) Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation or exclusion may not apply to you.

7. U.S. Government Restricted Rights. Use, duplication, or disclosure of the Software for or on behalf of the United States of America, its agencies and/or instrumentalities "U.S. Government" is subject to restrictions as stated in paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, or subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR supplement, as applicable.

8. General. This Agreement constitutes the entire understanding of the parties and revokes and supersedes all prior agreements, oral or written, between them and may not be modified or amended except in a writing signed by both parties hereto that specifically refers to this Agreement. This Agreement shall take precedence over any other documents that may be in conflict herewith. If any one or more provisions contained in this Agreement are held by any court or tribunal to be invalid, illegal, or otherwise unenforceable, each and every other provision shall remain in full force and effect.