William Panek
Microsoft MVP

MCSA

Windows 10

STUDY GUIDE

Exam 70-697

Covers 100% of Configuring Windows Devices exam objectives,
including installing Windows 10, storage and security, managing
data access, Microsoft Intune, identity and authorization,
network connectivity, recovery, and much more...
Includes online interactive learning environment with:

+ 2 custom practice exams
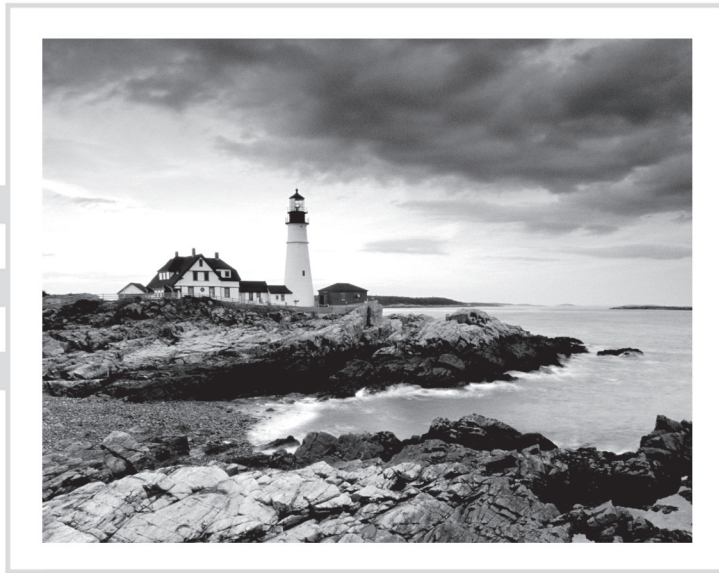+ More than 100 electronic flashcards
+ Searchable key term glossary

SYBEX®
A Wiley Brand

MCSA
Windows® 10

Study Guide
Exam 70-697

MCSA
Windows® 10
Study Guide
Exam 70-697

William Panek

SYBEX®
A Wiley Brand

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

10 9 8 7 6 5 4 3 2 1

This book is dedicated to the three ladies of my life: Crystal, Alexandria, and Paige.

Acknowledgments

About the Author

William Panek   holds the following certifications: MCP, MCP+I, MCSA, MCSA+ Security and Messaging, MCSE-NT (3.51 & 4.0), MCSE 2000, 2003, 2012/2012 R2, MCSE+Security and Messaging, MCDBA, MCT, MCTS, MCITP, CCNA, CCDA, and CHFI. Will is also a three-time and current Microsoft MVP winner.

   After many successful years in the computer industry, Will decided that he could better use his talents and his personality as an instructor. He began teaching for schools such as Boston University and the University of Maryland, just to name a few. He has done consulting and training for some of the biggest government and corporate companies in the world, including the United States Secret Service, Cisco, United States Air Force, and United States Army.

   In 2015, Will became a lead Microsoft instructor for StormWind Studios (http://www.stormwindstudios.com). He currently lives in New Hampshire with his wife and two daughters. Will was also a representative in the New Hampshire House of Representatives from 2010 to 2012. In his spare time, he likes to golf, ski, shoot, snowmobile, play racquetball, and ride his Harley. Will is also a commercially rated helicopter pilot.

Contents at a Glance

Contents

Table of Exercises

Introduction

This book was written from over 25 years of IT experience. I have taken that experience and translated it into a Windows 10 book that will help you not only prepare for the MCSA: Windows 10 Solutions Associate exams but also develop a clear understanding of how to install and configure Windows 10 while avoiding all the possible configuration pitfalls.

Many Microsoft books just explain the Windows operating system, but with *MCSA: Windows 10 Study Guide*, I go a step further, providing many in-depth, step-by-step procedures to support my explanations of how the operating system performs at its best.

Microsoft Windows 10 is the newest version of Microsoft's client operating system software. Microsoft has taken the best of Windows 7 and Windows 8 and combined them into the latest creation: Windows 10.

Windows 10 eliminates many of the problems that plagued the previous versions of Windows client, and it includes a much faster boot time and shutdown. It is also easier to install and configure, and it barely stops to ask the user any questions during installation. In this book, I will show you what features are installed during the automated installation and where you can make changes if you need to be more in charge of your operating system and its features.

This book takes you through all the ins and outs of Windows 10, including installation, configuration, online Microsoft subscriptions, auditing, backups, and so much more.

Windows 10 has improved on Microsoft's desktop environment, made networking easier, enhanced search ability, and improved performance—and that's only scratching the surface.

When all is said and done, this is a technical book for IT professionals who want to take Windows 10 to the next step and get certified. With this book, you will not only learn Windows 10 and hopefully pass the exams; you will also become a Windows 10 expert.

The Microsoft Certification Program

Since the inception of its certification program, Microsoft has certified more than two 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.

The Microsoft certification tracks for Windows 10 include the following:

Microsoft Certified Solutions Associate (MCSA): Windows 10   The MCSA is now the highest-level certification you can achieve with Microsoft in relation to Windows 10. It requires passing exam 70-697. This book assists in your preparation for the exam.

Microsoft Certified Technology Associate (MTA)   This is Microsoft's newest certification program. This certification targets those new to the IT field and tests candidates on the core competencies necessary to become an IT professional.

Microsoft Certified Technology Specialist (MCTS)   The MCTS certification program targets specific technologies instead of specific job roles. You must take and pass one to three exams.

Microsoft Certifies Solutions Expert (MCSE): Server Infrastructure or MCSE: Desktop Infrastructure   The MCSE certifications, in relation to Windows Server 2012 R2, require that you become a Windows Server MCSA first and then pass two additional exams. The additional exams will vary depending on which of the two MCSE tracks you choose. For more information, visit Microsoft's website at www.microsoft.com/learning.

How Do You Become Certified on Windows 10?

Attaining 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 should 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 10, you can prepare yourself well for the exam by using the proper tools. By working through this book, you can successfully meet the requirements to pass the Windows 10 exams.

MCSA Exam Requirements

Candidates for MCSA certification on Windows 10 must pass the Windows 10 MCSA test 70-697: Configuring Windows Devices.

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) for the most current listing of exam objectives. The published objectives and how they map this book are listed later in this introduction.

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.

Types of Exam Questions

In an effort to both refine the testing process and protect the quality of its certifications, Microsoft has focused its latest 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.

> **NOTE** 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. Let's take a look at the types of exam questions, so you'll be prepared for all of the possibilities.

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. 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.

> **NOTE** 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.

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.

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.

Tips for Taking the Windows 10 Exams

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. Do not be tempted to jump to an early conclusion. Make sure that you know *exactly* what the question is asking.
- Answer all questions. If you are unsure about a question, mark it for review and come back to it 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 that 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

At the time this book was released, Microsoft exams are given using more than 1,000 Authorized VUE Testing Centers around the world. For the location of a testing center near you, go to VUE's website at www.vue.com. If you are outside the United States and Canada, contact your local 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 $150 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.

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.

Microsoft requires certification candidates to accept the terms of a nondisclosure agreement before taking certification exams.

Who Should Read This Book?

This book is intended for individuals who want to earn their MCSA: Windows 10 certification.

This book will not only help anyone who is looking to pass the Microsoft exams; it will also help anyone who wants to learn the real ins and outs of the Windows 10 operating system.

What's Inside?

Here is a glance at what's in each chapter:

Chapter 1: Installing Windows 10   In the first chapter, I explain the requirements and steps to install and configure Windows 10. I also show you the different versions of Windows 10.

Chapter 2: Automated Windows 10 Deployments   This chapter shows you how to configure automated installation of Windows 10. I also explain Hyper-V and how imaging works. I also show you how to configure Mobility options.

Chapter 3: Configuring Storage and Security   I take you through the advantages and benefits of using NTFS over FAT32. I also show you how to configure and install hard drives and volumes.

Chapter 4: Managing Data Access   I show you how to configure shares and NTFS security. I also take you through the advantages of using BitLocker and BitLocker To Go.

Chapter 5: Managing the Windows 10 Environment   This chapter takes you through the different ways to configure the Windows 10 environment including remote connections, mobile computing, and power options.

Chapter 6: Planning and Managing Microsoft Intune   You will see how to manage and configure Microsoft Intune. I show you how to enroll devices into Intune and how to manage software using Intune.

Chapter 7: Configuring Applications   I show you how to manage and configure Windows applications including using virtual applications. I also demonstrate how to configure cloud-based applications.

Chapter 8: Managing Identity and Authorization   This chapter shows you how to configure users and groups. I teach you the different user and group types and how to create and manage those objects.

Chapter 9: Configuring Network Connectivity   This chapter shows you how to implement and configure Windows networking including workgroups and domains. I also talk about HomeGroups and how to configure TCP/IP.

Chapter 10: Configuring Recovery   This chapter explains how to implement and configure Windows backups and recovery points. I show you how to use cloud-based backups and how to recover the Windows 10 system using advanced boot options.

What's Included with the Book

There are many helpful items intended to prepare you for the MCSA: Windows 10 certification included in this book. These items include:

Assessment Test   There is an assessment test at the conclusion of the introduction that can be used to quickly evaluate where you are with Windows 10. This test should be taken prior to beginning your work in this book and should help you identify areas that you are either strong or weak in. Note that these questions are purposely simpler than the types of questions you may see on the exams.

Objective Map and Opening List of Objectives   At the beginning of the book, I have included a detailed exam objective map showing you where each of the exam objectives is covered. In addition, each chapter opens with a list of the exam objectives it covers. Use these resources to see exactly where each of the exam topics is covered.

Helpful Exercises   Throughout the book, I have included step-by-step exercises of some of the more important tasks you should be able to perform. Some of these exercises have corresponding videos that can be downloaded from the book's website. Also, I have included a recommended home lab setup, which will be helpful in completing these tasks.

Video Resources   After each chapter summary, if the chapter includes exercises with corresponding videos, a list or description of the exercises with video resources will be provided. The videos can be accessed at www.wiley.com/go/sybextestprep on the Other Study Tools tab.

Exam Essentials   The end of each chapter also includes a list of exam essentials. These are essentially repeats of the objectives, but remember that any objective on the exam blueprint could show up on the exam.

Chapter Review Questions   Each chapter includes review questions. These are used to assess your understanding of the chapter and are taken directly from the chapter. These questions are based on the exam objectives and are similar in difficulty to items you might actually receive on the MCSA: Windows 10 exams.

> **NOTE**
>
> The Sybex Interactive Online Test Bank, flashcards, videos, and glossary can be accessed at www.wiley.com/go/sybextestprep.

Interactive Online Learning Environment and Test Bank

The interactive online learning environment that accompanies *MCSA: Microsoft Windows 10 Study Guide: Exam 70-697* provides a test bank with study tools to help you prepare for the certification exams and increase your chances of passing them the first time! The test bank includes the following elements:

Sample Tests   All of the questions in this book are provided, including the assessment test, which you'll find at the end of this introduction, and the chapter tests that include the review questions at the end of each chapter. In addition, there are two practice exams. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices.

Electronic Flashcards   One set of questions is provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Glossary   The key terms from this book and their definitions are available as a fully searchable PDF.

Videos   Some of the exercises include corresponding videos. These videos show you how I do the exercises. There is also a video that shows you how to set up virtualization so that you can complete the exercises within a virtualized environment. I also have videos to help you on the Microsoft exams at www.youtube.com/c/williampanek.

Recommended Home Lab Setup

To get the most out of this book, you will want to make sure that you complete the exercises throughout the chapters. To complete the exercises, you will need one of two setups. First, you can set up a machine with Windows 10 and complete the labs using a regular Windows 10 machine.

The second way to set up Windows 10 is by using virtualization. I set up Windows 10 as a virtual hard disk (VHD), and I did all the labs this way. The advantage of using virtualization is that you can always just wipe out the system and start over without losing a real server. Plus, you can set up multiple virtual servers and create a full lab environment on one machine.

I created a video for this book showing you how to set up a virtual machine and how to install Windows 10 onto that virtual machine. This video can be seen at www.youtube .com/c/williampanek.

How to Contact Sybex or the Author

Sybex strives to keep you supplied with the latest tools and information you need for your work. Please check the website at www.sybex.com/go/mcsawin10, where I'll post additional content and updates that supplement this book should the need arise.

You can contact Will Panek by going to www.willpanek.com. Will Panek also has videos and test prep information located at www.youtube.com/c/williampanek. Will also has a Windows 10 Facebook page and a Twitter account, @AuthorWillPanek.

MCSA Microsoft Windows 10: Exam 70-697 Objectives Map

The following table provides a breakdown of this book's exam coverage, listing the chapter where each objective and its subobjectives are covered:

Objective	Chapter
1. Manage identity	
Support Windows Store and cloud apps	**Chapter 6, Chapter 7**
Install and manage software by using Microsoft Office 365 and Windows Store apps	
Sideload apps by using Microsoft Intune	
Sideload apps into online and offline images	
Deeplink apps by using Microsoft Intune	
Integrate Microsoft account including personalization settings	

Objective	Chapter
Support authentication and authorization	**Chapter 8**
Identifying and resolving issues related to the following: Multi-factor authentication including certificates, Microsoft Passport, virtual smart cards, picture passwords, and biometrics; workgroup vs. domain, Homegroup, computer and user authentication including secure channel, account policies, credential caching, and Credential Manager; local account vs. Microsoft account; Workplace Join; Configuring Windows Hello	
2. Plan desktop and device deployment	
Migrate and configure user data	**Chapter 1**
Migrate user profiles	
Configure folder location	
Configure profiles including profile version, local, roaming, and mandatory	
Configure Hyper-V	**Chapter 2**
Create and configure virtual machines including integration services	
Create and manage checkpoints	
Create and configure virtual switches	
Create and configure virtual disks	
Move a virtual machine's storage	
Configure mobility options	**Chapter 5**
Configure offline file policies	
Configure power policies	
Configure Windows To Go	
Configure sync options	
Configure Wi-Fi direct, files, powercfg, Sync Center	
Configure security for mobile devices	**Chapter 4**
Configure BitLocker	
Configure startup key storage	
3. Plan and implement a Microsoft Intune device management solution	
Support mobile devices	**Chapter 6**
Support mobile device policies including security policies, remote access, and remote wipe	
Support mobile access and data synchronization including Work Folders and Sync Center	
Support broadband connectivity including broadband tethering and metered networks	
Support Mobile Device Management by using Microsoft Intune, including Windows Phone, iOS, and Android	

Objective	Chapter
Deploy software updates by using Microsoft Intune	**Chapter 6**
Use reports and In-Console Monitoring to identify required updates, approve or decline updates, configure automatic approval settings, configure deadlines for update installations, deploy third-party updates	
Manage devices with Microsoft Intune	**Chapter 6**
Provision user accounts	
Enroll devices	
View and manage all managed devices	
Configure the Microsoft Intune subscriptions	
Configure the Microsoft Intune connector site system role	
Manage user and computer groups	
Configure monitoring and alerts	
Manage policies	
Manage remote computers	
4. Configure networking	
Configure IP settings	**Chapter 9**
Configure name resolution	
Connect to a network	
Configure network locations	
Configure networking settings	**Chapter 9**
Connect to a wireless network	
Manage preferred wireless networks	
Configure network adapters	
Configure location-aware printing	
Configure and maintain network security	**Chapter 9**
Configure Windows Firewall	
Configure Windows Firewall with Advanced Security	
Configure connection security rules (IPsec)	
Configure authenticated exceptions	
Configure network discovery	
5. Configure storage	
Support data storage	**Chapter 3**
Identifying and resolving issues related to the following: DFS client including caching settings, storage spaces including capacity and fault tolerance, OneDrive	

Objective	Chapter
Support data security	**Chapter 3, Chapter 4**
Identifying and resolving issues related to the following: Permissions including share, NTFS, and Dynamic Access Control (DAC)	
Encrypting File System (EFS) including Data Recovery Agent	
Access to removable media	
BitLocker and BitLocker To Go including Data Recovery Agent and Microsoft BitLocker Administration and Monitoring (MBAM)	
6. Manage data access and protection	
Configure shared resources	**Chapter 4**
Configure shared folder permissions	
Configure HomeGroup settings	
Configure libraries	
Configure shared printers	
Configure OneDrive	
Configure file and folder access	**Chapter 3**
Encrypt files and folders by using EFS	
Configure NTFS permissions	
Configure disk quotas	
Configure file access auditing	
Configure authentication and authorization	
7. Manage remote access	
Configure remote connections	**Chapter 5**
Configure remote authentication	
Configure Remote Desktop settings	
Configure VPN connections and authentication	
Enable VPN reconnect	
Configure broadband tethering	
Configure mobility options	**Chapter 5**
Configure offline file policies	
Configure power policies	
Configure Windows To Go	
Configure sync options	
Configure Wi-Fi direct, files, powercfg, Sync Center	

Objective	Chapter
8. Manage apps	
Deploy and manage Azure RemoteApp	**Chapter 7**
Configure RemoteApp and Desktop Connections settings	
Configure Group Policy Objects (GPOs) for signed packages	
Subscribe to the Azure RemoteApp and Desktop Connections feeds	
Export and import Azure RemoteApp configurations	
Support iOS and Android	
Configure remote desktop web access for Azure RemoteApp distribution	
Support desktop apps	**Chapter 6, Chapter 7**
The following support considerations including: Desktop app compatibility using Application Compatibility Toolkit (ACT) including shims and compatibility database; desktop application co-existence using Hyper-V, Azure RemoteApp, and App-V; installation and configuration of User Experience Virtualization (UE-V); deploy desktop apps by using Microsoft Intune	
9. Manage updates and recovery	
Configure system recovery	**Chapter 10**
Configure a recovery drive	
Configure system restore	
Perform a refresh or recycle	
Perform a driver rollback	
Configure restore points	
Configure file recovery	**Chapter 10**
Restore previous versions of files and folders	
Configure File History	
Recover files from OneDrive	
Configure and manage updates	**Chapter 1**
Configure update settings	
Configure Windows Update policies	
Manage update history	
Roll back updates	
Update Windows Store apps	

NOTE

Exam domains and objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit their website (https://www.microsoft.com/en-us/learning/exam-70-697.aspx) for the most current information.

Assessment Test

1. What filename 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 10 computers?

   A. The user who uses the profile

   B. Server operators

   C. Power users

   D. Administrators

3. Your employees use both desktops and tablets to access the company network. Your tablet users use a 4G mobile broadband Wi-Fi connection. You need to monitor how much data your users are using for this connection. How do you accomplish this?

   A. Configure the broadband connection as a metered network.

   B. Turn on network resource monitoring.

   C. Enable Performance Monitor.

   D. Enable tablet metering in the tablets' settings.

4. If you wanted to require that a user enter an Administrator password to perform administrative tasks, 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 10 on your computer. You want to create an image of the new installation to use as a basis for remote installs. What Windows 10 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 10? (Choose all that apply.)

    A. The built-in Administrator account does not exist in Windows 10.

    B. The built-in Administrator account is disabled by default in Windows 10.

    C. The built-in Administrator account has no permissions in Windows 10.

    D. The built-in Administrator account is not a member of the Administrators group in Windows 10.

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 10 preinstalled. You want to migrate existing users from a 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. `Windows7Migrate.exe`

9. You are the IT director for large company that has decided to move to the cloud. The company wants to use Azure Active Directory and Microsoft Intune. The company has been looking into this because users have been using multiple devices to get their job done. When your users get added to Intune and get licensed, how many devices can each user add by default?

    A. Three

    B. Four

    C. Five

    D. None. Device administrators are the only persons who can add devices to Intune.

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 10 computer has been infected with spyware. You remove the spyware from her computer and want to prevent spyware from infecting it in the future. Which of the following Windows 10 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 subscribe to. One of the feeds stores only the 10 most recent updates. 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 updated 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. What is the CIDR equivalent for **255.255.255.224**?

   A. /24

   B. /25

   C. /26

   D. /27

15. You are configuring a new Windows 10 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? (Choose all that apply.)

   A. Install a printer.

   B. Install network drivers.

   C. Configure WPA keys.

   D. Modify the Desktop settings.

16. You are the network administrator for Stellacon. Your network consists of 200 Windows 10 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 10 Home. 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 10 Enterprise.

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. `DNS /flushdns`

19. Which of the following information can be configured on a VPN client so that it can access a VPN server? (Choose two.)

A. IP address

B. MAC address

C. Domain name

D. Connection address

20. Which of the following statements are true regarding the creation of a group in Windows 10? (Choose two.)

A. Only members of the Administrators group can create users on a Windows 10 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 10 computer. You are considering using spanned volumes. Which of the following statements 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. You have just installed Hyper-V on a server called ServerA and you have set up five new VM servers. You want to run PowerShell commands for the five VM servers from ServerA. How do you do this?

A. Use the `Invoke-Command` cmdlet and specify the `VMName` parameter.

B. Use the WinRM command `-PowerShell`.

C. Use the `PSCommands - enabled` command.

D. Just run the PowerShell commands with the `-Name` parameter.

23. Your home computer network is protected by a firewall. You have configured your Windows 10 home computer to use Windows Mail. After you configure your email accounts, you discover that you are unable to send email messages from Windows Mail. Your email provider uses POP3 and SMTP. What port should you open on the firewall?

A. 25

B. 110

C. 443

D. 995

24. You need Windows 10 to be the primary operating system on a dual-boot machine. Which file do you configure for this?

A. `boot.ini`

B. `bcdedit`

C. `bcboot.ini`

D. `bcdboot`

25. Which of the following versions of Windows 10 can be upgraded to Windows 10 Enterprise edition? (Choose all that apply.)

A. Windows 8 Home

B. Windows 8 Professional

C. Windows 8 Home Premium

D. Windows 8 Enterprise

26. You are configuring a Windows 10 computer that is going to be used by your children. You are configuring access restrictions using the Parental Controls feature of Windows 10. Which of the following can be configured by setting Parental Controls? (Choose all that apply.)

A. When your children can access the computer

B. Which websites your children can view

C. Which programs your children can access

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

27. How do you access the Advanced Boot Options menu in Windows 10 during the boot process?

A. Press the spacebar.

B. Press F6.

C. Press F8.

D. Press F10.

28. You have two remote sites with Windows 10 machines. You need to share data across the slow sites. What feature can help with this?

A. Link Detection

B. BranchCache

C. DirectAccess

D. DirectCache

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

A. UPFS

B. UPGRADE

C. Disk Manager

D. Convert

30. Your organization has created an application for its employees. You need to deploy the internally developed application to all employees while minimizing the costs. What's the best way to do that?

A. Install the application one system at a time.

B. Enable application sideloading.

C. Purchase System Center and deploy the application.

D. Run the `Add-Application` PowerShell cmdlet.

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 8 for more information.

3. **A.** Administrators have the ability to limit and monitor network usage by configuring the network as a metered network. Network metering allows network downloading to be watched or metered and then administrators can charge users or departments for the network usage. See Chapter 6 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 8 for more information.

5. **C.** You can use the ImageX utility to create an image of a Windows 10 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 10. See Chapter 2 for more information.

6. **B.** The built-in Administrator account is disabled by default in Windows 10. However, it can be enabled through Local Users and Groups or by modifying the Accounts: Administrator Account Status GPO setting. See Chapter 8 for more information.

7. **D.** The Narrator utility uses a sound output device to read onscreen text. See Chapter 5 for more information.

8. **B, C.** Windows 10 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 2 for more information.

9. **C.** By default, licensed users can add up to five devices to their accounts. Device administrators have the ability to add devices to Intune, but users do have the ability to enroll up to five devices on their own. See Chapter 6 for more information.

10. **C.** Internet Explorer 11 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 7 for more information.

11. **A.** Windows Defender is an antispyware program included with Windows 10. It 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 7 for more information.

12. **B.** Sleep mode is a combination of standby mode and hibernation 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 **10.** See Chapter 5 for more information.

13. D. Internet Explorer 11 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 7 for more information.

14. D. A subnet mask of 255.255.255.224 equals a CIDR of /27. CIDR is the number of on bits. See Chapter 9 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 8 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 to 254. See Chapter 9 for more information.

17. A. To enable synchronization of files between your laptop and a network folder, you must first upgrade your laptop to a version of Windows 10 that supports synchronization with network folders, such as Windows 10 Enterprise. Windows Sync Center also supports synchronization of files between computers and mobile devices. See Chapter 1 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 9 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 5 for more information.

20. A, C. Only administrators can create new groups on a Windows 10 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 8 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 10, 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 3 for more information.

22. A. Administrators can use PowerShell Direct to run PowerShell commands on a VM from the Hyper-V host. To do this, you need to run the following command, `Invoke-Command`, and you need to specify which VM you're connecting to (`-VMName` parameter). See Chapter 7 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 9 for more information.

24. B. You should configure the `bcdedit` utility to configure your boot order. See Chapter 1 for more information.

25. B, D. You can upgrade Windows 8 Professional and Windows 8 Enterprise to Windows 10 Enterprise edition. See Chapter 1 for more information.

26. A, B, C. Using Parental Controls, you can configure which websites your children can access, when they can use the computer, which games they can play, and which programs they can run, and you can view reports regarding their activity. See Chapter 5 for more information.

27. C. During the boot process, you are prompted to press F8 to access the Advanced Boot Options menu. See Chapter 10 for more information.

28. B. BranchCache allows multiple sites with slower links to share data quickly and efficiently. See Chapter 5 for more information.

29. D. The Convert utility is used to convert a FAT32 partition to NTFS. See Chapter 3 for more information.

30. B. Applications that are developed by a company and are not signed by the Windows Store can be installed by the process of sideloading. Sideloading allows companies to load applications into the Windows Store for deployment throughout a company. See Chapter 7 for more information.

Chapter

1

Installing Windows 10

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Migrate and configure user data.**

■ This objective may include but is not limited to the following subobjectives: migrate user profiles; configure folder location; configure profiles including profile version, local, roaming, and mandatory.

✓ **Configure and manage updates.**

■ This objective may include but is not limited to the following subobjectives: Configure update settings, configure Windows Update policies, manage update history, roll back updates, update Windows Store apps.

Welcome to Windows 10 and the future of Microsoft Windows computing. In previous editions of Microsoft Windows, Microsoft introduced the networking world to using the cloud for storage. Windows 10 starts to take this even further.

But let's start at the beginning. Before you can master any Microsoft product, you must know about the different versions of Windows 10 and also how to properly install Windows 10. In this chapter, I will show you the many different features of Windows 10 and describe each edition. I will then show you how to install Windows 10 and set up the user profiles. This is a straightforward process that can be highly automated and user friendly.

Preparing for the installation of Windows 10 involves making sure your hardware meets the minimum requirements and is supported by the operating system. Another consideration when installing Windows 10 is whether you are going to upgrade from a previous version of Windows or install 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.

To complete the Windows 10 installation, you will need to activate the product through Windows Activation. This process is used to reduce software piracy. After Windows 10 is installed, you can keep the operating system up-to-date with postinstallation updates.

Introducing Windows 10

Microsoft Windows 10 is the newest version of Microsoft's client operating system software. Windows 10 combines the best of Windows 7 and Windows 8.

At the time this book was written, Microsoft has currently released six different versions of the Windows 10 operating system:

- Windows 10 Home
- Windows 10 Professional
- Windows 10 Enterprise
- Windows 10 Education
- Windows 10 Mobility
- Windows 10 Mobility Enterprise

> **NOTE** Two of the versions listed previously will not be covered in this book, Windows 10 Mobility and Windows 10 Mobility Enterprise. If you go to Microsoft's website, you will see both listed and you can see what each offers. But neither of them can be put onto a network, so we don't cover them in this book.

Windows 10 has been improved in many of the weak areas that plagued Windows 8. Windows 10 has a much faster boot time and shutdown compared to Windows 8. It also brings back the previous Start button that we are all so familiar with from previous editions.

The Windows 10 operating system functions are also faster than their previous counterparts. The processes for opening, moving, extracting, compressing, and installing files and folders are more efficient than they were in previous versions of Microsoft's client operating systems.

Let's take a look at some of the features of each Windows 10 edition (this is just an overview of some of the benefits to using Windows 10). Table 1.1 shows each edition and what some of the "core experiences" are for those editions.

> **NOTE** The information in Table 1.1 and Table 1.2 was taken directly from Microsoft's website.

TABLE 1.1   Windows 10 Core Experiences

Feature	Home	Pro	Enterprise	Education
Battery saver	●	●	●	●
Built-in ink support	●	●	●	●
Cortana integration	●	●	●	●
Customizable Start Menu	●	●	●	●
Enterprise-level biometric security	●	●	●	●
Fast startup with Hiberboot and InstantGo	●	●	●	●
"Hey Cortana" hands-free activation	●	●	●	●
Native facial and iris recognition	●	●	●	●
Native fingerprint recognition	●	●	●	●

TABLE 1.1   Windows 10 Core Experiences *(continued)*

Feature	Home	Pro	Enterprise	Education
Personal and proactive suggestions	●	●	●	●
Reading view	●	●	●	●
Reminders	●	●	●	●
Search web, device, and cloud	●	●	●	●
Snap apps (across screens on different monitors)	●	●	●	●
Snap assist (up to four apps on one screen)	●	●	●	●
Switch from PC to tablet mode	●	●	●	●
Talk or type naturally	●	●	●	●
TPM support	●	●	●	●
Virtual desktops	●	●	●	●
Windows Defender and Windows Firewall	●	●	●	●
Windows Update	●	●	●	●

Now that we've looked at some of the Windows 10 core experiences, let's take a look at the business side. Table 1.2 shows each edition and what some of the "Business Experiences" are for those editions.

TABLE 1.2   Windows 10 Business Experiences

Feature	Home	Pro	Enterprise	Education
Ability to join Azure Active Directory		●	●	●
AppLocker			●	●
Assigned Access 8.1		●	●	●
BitLocker		●	●	●
BranchCache			●	●

Feature	Home	Pro	Enterprise	Education
Client Hyper-V		●	●	●
Credential Guard			●	●
Current Branch for Business		●	●	●
Device Encryption	●	●	●	●
Device Guard			●	●
Direct Access			●	●
Domain Join		●	●	●
Easy Upgrade from Home to Education Edition	●	●		●
Easy Upgrade from Pro to Enterprise Edition		●	●	
Enterprise Data Protection		●	●	●
Enterprise Mode Internet Explorer (EMIE)		●	●	●
Granular UX Control			●	●
Group Policy Management		●	●	●
Long Term Servicing Branch			●	
Microsoft Passport	●	●	●	●
Mobile device management	●	●	●	●
Remote Desktop		●	●	●
Side-loading of line-of-business apps	●	●	●	●
Start Screen Control with Group Policy			●	●
Trusted Boot		●	●	●
Windows Store for Business		●	●	●
Windows To Go Creator			●	●
Windows Update	●	●	●	●
Windows Update for Business		●	●	●

Windows 10 Features

Now that we have seen which editions contain which features, let's take a look at some of the Windows 10 features in greater detail. This section describes only a few of these features, but all features will be explained throughout this book.

Cortana Integration   Windows 10 comes with Cortana integration. Cortana is your very own personnel assistant. You can type in or ask Cortana a question, and Cortana will seek out the best possible answer based on your question.

Secure Boot   Windows 10 gives you the ability to use hardware-based virtualization that allows Windows 10 to prevent malware from running on your system. Windows 10 Secure Boot also prevents key processes from being tampered with because Windows 10 isolates these processes from the system.

Enterprise Data Protection   Windows 10 Enterprise Data Protection (EDP) helps protect corporate data in a world that is increasingly becoming a Bring Your Own Device (BYOD) environment. Since many organizations are allowing employees to connect their own devices to their network, the possibility of corporate data being compromised because of non-corporate programs running on these personnel devices is increasing. For example, many third-party apps may put corporate data at risk by accidently disclosing corporate information through the application.

Enterprise Data Protection helps protect information by separating corporate applications and corporate data from being disclosed by personal devices and personal applications.

Device Guard   Because employees can use multiple types of Windows 10 devices (Surface Pros, Windows Phones, and Windows 10 computer systems), Device Guard is a feature that helps guarantee that only trusted applications will run on any of these devices.

Device Guard uses both hardware and software security features to lock down a device so it can run only trusted and approved applications. This also helps protect against hackers from running malicious software on these devices.

Microsoft Passport   Windows 10 allows administrators to replace passwords with other types of authentication on the operating system. Microsoft Passport allows for multifactor authentication by using a combination of an enrolled device and biometric authentication or a personal identification number (PIN).

Microsoft has encompassed the use of your Microsoft account with the use of your corporate account. So with Windows 10, Microsoft Passport can log you into your domain as well as into the cloud and Microsoft websites. The user will be required to verify their Microsoft Passport account, and that account will then be tied into a gesture or PIN, and from that point on, the user will not need to use a password to log in to the device and their protected resources. Because no password will be needed, this helps prevent hackers from using software to hack a password on an account.

Start Menu   Windows 10 has brought back the Start Menu that users are familiar with. The Windows 10 Start Menu combines the best of both Windows 7 and Windows 8. So the Start Menu gives you a menu that we were familiar with in Windows 7 as well as the Live Tiles that users liked in Windows 8.

Microsoft Edge and Internet Explorer 11   Windows 10 has introduced a new way to surf the Internet with Microsoft Edge. But Windows 10 also still comes with Internet Explorer 11 in the event that you need to run ActiveX controls or run backward-compatible web services or sites.

Microsoft Edge allows users to start using many new Microsoft features, including Web Note (allows you to annotate, highlight, and call things out directly on web pages), Reading View (allows you to print and save as a PDF for easy reading), and Cortana (personal assistant).

Domain Join and Group Policy   Depending on the version of Windows 10 that you are using, administrators have the ability to join Windows 10 clients to either a corporate version of Active Directory or a cloud-based version of Azure Active Directory.

Windows Store for Business   Microsoft Store has included many applications that allow users to get better functionality and productivity out of their Windows 10 devices. One advantage for corporations is that they can create their own applications and load them into the Microsoft Store for users to download (called *sideloading*).

Mobile Device Management   Mobile Device Management (MDM) allows administrators to set up Windows 10 policies that can integrate many corporate scenarios, including the ability to control users' access to the Windows Store and the ability to use the corporate VPN. MDM also allows administrators to manage multiple users who have accounts set up on Microsoft Azure Active Directory (Azure AD). Windows 10 MDM support is based on the Open Mobile Alliance (OMA) Device Management (DM) protocol 1.2.1 specification.

🌐 Real World Scenario

Choosing an Appropriate Operating System

As an IT consultant, I have clients who want to stay on the leading edge of technology but don't have the money to replace all of their equipment. This is where I have to convince the client that it is better to slowly migrate their equipment.

Try presenting a timeline to your customers or organization that shows the migration to Windows 10. Your clients will be happy, and you will have the time needed to migrate your organization.

I understand that if you are reading this book, there is the strong likelihood that you are getting ready to install or upgrade to Windows 10 in your organization.

Microsoft has taken the best of Windows 7 and Windows 8 and created Windows 10. In a corporate environment, if you have machines running Windows 8, most will have a free upgrade to Windows 10, which will improve performance. But if you have clients who are comfortable and happy with Windows 7, a decision will need to be made about whether to stay with Windows 7 or upgrade to Windows 10.

Windows Feature Deprecation

With the release of its newest operating system, Microsoft has decided that some of the features you may be used to are no longer needed. Here are some of the features that have been deprecated:

- Windows 7 desktop gadgets will be removed as part of Windows 10.
- The Solitaire, Minesweeper, and Hearts games that come preinstalled on Windows 7 will be removed. Microsoft has released versions of Solitaire and Minesweeper called the "Microsoft Solitaire Collection" and "Microsoft Minesweeper."
- Mobile Device Management functionality will not be available in Windows 10 Home edition.
- Users with floppy drives will need to download the latest driver from Windows Update or from the manufacturer's website.
- Users who have Windows Live Essentials installed on their systems will lose the One-Drive application, which will be replaced with the inbox version of OneDrive.
- OneDrive will no longer support placeholder files in Windows 10. Windows 10 users can choose which folders they want to sync from OneDrive settings.
- When upgrading Windows 10 with versions of previous operating systems that support Media Center, Windows Media Center will be removed. For a limited time on systems that were upgraded to Windows 10 from one of these versions of Windows, a DVD playback app, Windows DVD Player, will be installed. If the Windows DVD Player does not install immediately, it will be installed after the first successful Windows update.

Windows 10 Architecture

Windows 10 has limited the number of files that load at system startup to help with the core performance of the operating system. Microsoft has also removed many of the fluff items that Windows Vista used, allowing for better performance.

Microsoft offers both a 32-bit version and a 64-bit version of Windows 10. The terms *32-bit* and *64-bit* refer to the CPU, or processor. The number represents how the data is processed. It is processed either as 2^{32} or 2^{64}. The larger the number, the larger the amount of data that can be processed at any one time.

To get an idea of how 32-bit and 64-bit processors operate, think of a large highway with 32 lanes. Vehicles can travel on those 32 lanes only, so when traffic gets backed up, the result is delays. Now think of how many more vehicles can travel on a 64-lane highway. The problem here is that a 32-lane highway can't handle the number of vehicles a 64-lane highway can. You need to have the infrastructure to allow for that volume of vehicles. The same is true for computers. Your computer has to be configured to allow you to run a 64-bit processor.

So what does all of this mean to the common user or administrator? It's all about random access memory, or RAM. A 32-bit operating system can handle up to 4 GB of RAM, and a 64-bit processor can handle up to 16 exabytes of RAM. None of this is new. Although 64-bit processors are just starting to get accepted with Windows systems, other operating systems, such as Apple, have been using 64-bit processors for many years.

> **NOTE** 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 1 second. This measurement is typically expressed in gigahertz (GHz). One GHz is one billion 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.

Now that you have seen the new features of Windows 10, let's look at how to prepare the machine to install Windows 10.

Preparing to Install Windows 10

Installing Windows 10 can be relatively simple because of the installation wizard. The installation wizard will walk you through the entire installation of the operating system.

The most difficult part of installing Windows 10 is preparing and planning for the installation. One thing I often say to IT professionals is, "An hour of planning will save you days of work." Planning a Windows 10 rollout is one of the hardest and most important tasks that you will perform when installing Windows 10.

There are many decisions that should be made before you install Windows 10. The first decision is which version of Windows 10 you want to install. As mentioned previously, Microsoft has six different versions of the Windows 10 operating system. This allows an administrator to custom-fit a user's hardware and job function to the appropriate version of Windows 10. Many times, Microsoft releases multiple editions of the operating system

contained within the same Windows 10 media disk. You can choose to unlock the one you want based on the product key you have. Let's take a closer look at the different versions of Windows 10.

> **NOTE** In this book, we will not talk much about Windows 10 Education. Windows 10 Education is the counterpart to Windows 10 Enterprise, but it is a volume-licensed version of Windows 10 that is specifically priced for educational institutions. Educational institutions receive the same Enterprise functionality, but they pay much less than a corporation.

Windows 10 Home

Windows 10 Home is the main operating system for home users. Windows 10 Home offers many features, including these:

- Broad application and device compatibility with unlimited concurrent applications
- A safe, reliable, and supported operating system
- Microsoft Passport
- HomeGroup, which allows a user to easily share media, documents, and printers across multiple PCs in homes or offices without the need of a domain
- Improved Taskbar and Jump Lists (Jump Lists is a feature in Windows 10 that allows you to quickly access files that you have been working on.)
- Live thumbnail previews and an enhanced visual experience
- Advanced networking support (ad hoc wireless networks and Internet connection sharing)
- View Available Networks (VAN) (Windows 10 by default has the ability, when you use a wireless network adapter, to choose the wireless network that you want to connect to by using the wireless network adapter properties.)
- Device Encryption
- Easy networking and sharing across all your PCs and devices
- Windows Update
- Multitouch
- Improved handwriting recognition

Windows 10 Professional

Windows 10 Professional is designed for small-business owners. Microsoft designed Windows 10 Professional for users to get more done and safeguard their data. Professional offers the following features:

- Broad application and device compatibility with unlimited concurrent applications
- A safe, reliable, and supported operating system
- Microsoft Passport
- Domain Join
- Improved Taskbar and Jump Lists
- Enterprise Mode Internet Explorer (EMIE)
- Advanced networking support (ad hoc wireless networks and Internet connection sharing)
- View Available Networks (VAN) (Windows 10 by default has the ability, when you use a wireless network adapter, to choose the wireless network that you want to connect to by using the wireless network adapter properties.)
- Mobility Center
- Action Center, which makes it easier to resolve many IT issues yourself
- Easy networking and sharing across all your PCs and devices
- Group Policy Management
- Windows Update and Windows Update for Business
- Multitouch
- Improved handwriting recognition
- Domain Join, which enables simple and secure server networking
- BitLocker, which protects data on removable devices
- Device Encryption
- Encrypting File System, which protects data
- Client Hyper-V
- Location Aware Printing, which helps find the right printer when moving between the office and home
- Start Menu that includes Live Tiles

Windows 10 Enterprise

Windows 10 Enterprise is the version designed for midsize and large organizations. This operating system has the most features and security options of all Windows 10 versions. Here are some of the features:

- Broad application and device compatibility with unlimited concurrent applications.
- A safe, reliable, and supported operating system.
- Microsoft Passport.
- Enterprise Mode Internet Explorer (EMIE).

- Group Policy Management.

- Windows Update and Windows Update for Business.

- Advanced networking support (ad hoc wireless networks and Internet connection sharing).

- View Available Networks (VAN). Windows 10 by default has the ability, when you use a wireless network adapter, to choose the wireless network that you want to connect to by using the wireless network adapter properties.

- Mobility Center.

- Easy networking and sharing across all your PCs and devices.

- Multitouch.

- Start menu that includes Live Tiles.

- Improved handwriting recognition.

- Domain Join, which enables simple and secure server networking.

- Device Encryption.

- Encrypting File System, which protects data.

- Location Aware Printing, which helps find the right printer when you are moving between the office and home.

- Client Hyper-V.

- Credential Guard.

- Device Guard.

- BitLocker, which protects data on removable devices.

- DirectAccess, which links users to corporate resources from the road without a virtual private network (VPN).

- BranchCache, which makes it faster to open files and web pages from a branch office.

- AppLocker, which restricts unauthorized software and also enables greater security hardware requirements

Before you can install the operating system, you must make sure the machine's hardware can handle the Windows 10 operating system.

To install Windows 10 successfully, your system must meet or exceed certain hardware requirements. Table 1.3 lists the minimum requirements for a Windows 10–capable PC.

TABLE 1.3   Hardware requirements

Component	Requirements
CPU (processor)	1 GHz or faster processor or system-on-a-chip (SoC)
Memory (RAM)	1 GB for 32-bit or 2 GB for 64-bit

Component	Requirements
Hard disk	16 GB for 32-bit OS 20 GB for 64-bit OS
Video adapter	DirectX 9 or later with WDDM 1.0 driver
Optional drive	DVD-R/W drive
Network device	Compatible network interface card

The hardware requirements listed in Table 1.3 are those specified at the time this book was written. Always check the Microsoft website for the most current information.

The Windows 10–capable PC must meet or exceed the basic requirements to deliver the core functionality of the Windows 10 operating system. These requirements are based on the assumption 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. Remember, the better the hardware, the better the performance.

Real World Scenario

Deciding on Minimum Hardware Requirements

The company you work for has decided that everyone will have their own laptop running Windows 10. 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 email 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, a 1 GHz Celeron processor and 1 GB of RAM will make for a very slow-running machine. So for this usage, you can assume that the minimum baseline configuration would be higher than a 1 GHz processor with at least 2 GB 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 of whether the RAM and processor calculations you have made for your environment are going to provide a 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 written, 500 GB 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.

The requirements for the graphics card depend on the resolution at which you want to run. The required amount of memory is as follows:

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

Measurement Used for Disk Space and Memory

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

- 1 MB (megabyte) = 1,024 KB (kilobytes)

- 1 GB (gigabyte) = 1,024 MB

- 1 TB (terabyte) = 1,024 GB

- 1 PB (petabyte) = 1,024 TB

- 1 EB (exabyte) = 1,024 PB

If you are not sure if your machine meets the minimum requirements, Microsoft includes some tools that can help you determine if a machine is Windows 10 compatible, which we will look at in the following sections.

The Hardware Compatibility List

Along with meeting the minimum requirements, whenever possible 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 10 operating system. To determine if your computer and peripherals are on the HCL, check the most up-to-date list at

```
https://msdn.microsoft.com/en-us/library/windows/hardware/
dn922588(v=vs.85).aspx
```

The Windows 10 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 10. Microsoft guarantees that the items on the list meet the requirements for Windows 10 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.

BIOS Compatibility

Before you install Windows 10, you should verify that your computer has the most current BIOS. 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 10 to function properly. Check the computer vendor's website for the latest BIOS version information.

Driver Requirements

To successfully install Windows 10, you must have the critical device drivers for your computer, such as the hard drive device driver. The Windows 10 media come with an extensive list of drivers. If your computer's device drivers are not on the Windows 10 installation media, you should check the device manufacturer's website.

New 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 Vista, you are eligible to use an upgrade copy of Windows 10.

The bad news is that if you are moving from Windows Vista, Windows XP, or earlier versions of Windows to Windows 10, you must perform a clean install. (You can, however, use the Windows Easy Transfer utility to migrate files and settings from Windows XP to Windows 10 on the same computer.)

You can perform an upgrade to Windows 10 if the following conditions are true:

- You are running Windows 7 or Windows 8.
- 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 of Windows 10 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 10 (such as DOS, Windows 9*x*, Windows NT, Windows Me, Windows 2000 Professional, Windows Vista, or Windows XP).
- You want to start from scratch, without keeping any existing preferences.
- You want to be able to dual-boot between Windows 10 and your previous operating system.

Table 1.4 shows each operating system that can be upgraded and the edition of Windows 10 to which it should be upgraded.

TABLE 1.4 Windows 7 and Windows 8 upgrade options

From Current Edition	Windows 10 Edition
Windows 7 Starter	Windows 10 Home
Windows 7 Home Basic	Windows 10 Home
Windows 7 Home Premium	Windows 10 Home
Windows 7 Professional	Windows 10 Pro
Windows 7 Ultimate	Windows 10 Pro
Windows 7 Enterprise	Windows 10 Enterprise
Windows Phone 8.1	Windows 10 Mobile
Windows 8.1 Home	Windows 10 Home
Windows 8.1 Pro	Windows 10 Pro
Windows 8.1 Enterprise	Windows 10 Enterprise
Windows 8.1 Pro for Students	Windows 10 Pro

Upgrade Considerations

Almost all Windows 7 and Windows 8 applications should run with the Windows 10 operating system. However, possible exceptions to this statement include the following:

- Applications that use file-system filters, such as antivirus software, may not be compatible.
- Custom power-management tools may not be supported.

Before upgrading to Windows 10, be sure to stop any antivirus scanners, network services, or other client software. These software packages may see the Windows 10 install as a virus and cause installation issues.

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.

Hardware Compatibility Issues

You need to ensure that you have Windows 10 device drivers for your hardware. If you have a video driver without a Windows 10–compatible driver, the Windows 10 upgrade will install the Standard VGA driver, which will display the video with an 800×600 resolution. Once you get the Windows 10 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 10. After the upgrade, if you have application problems, you can address the problems in any of the following ways:

- If the application is compatible with Windows 10, 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) to determine the compatibility of your current applications with Windows 10. 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 10, use the Windows 10 Program Compatibility Wizard. From the Control Panel, click the Programs icon, and then click the Run Programs From Previous Versions link to start the Program Compatibility Wizard. If the application is not compatible with Windows 10, upgrade your application to a Windows 10–compliant version.

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 7 or Windows 8) will help you plan and implement a successful upgrade strategy:

- Verify that your computer meets the minimum hardware requirements for Windows 10.

- Be sure your hardware is on the HCL.

- Make sure you have the Windows 10 drivers for the hardware. You can verify this with the hardware manufacturer.

- To audit the current configuration and status of your computer, run the Get Windows 10 App tool from the Microsoft website, which also includes documentation on using the utility. 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 10.

- Make sure your BIOS is current. Windows 10 requires that your computer has the most current BIOS. If it does not, it 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 because 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. Likewise, if you don't have a valid backup, you will likely 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 hard 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 hard drive for the upgrade.

- Perform the upgrade. In this step, you upgrade from the Windows 7 or Windows 8 operating system to Windows 10.

- Verify your configuration. After Windows 10 has been installed, use the inventory to compare and test each element that was 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, I have made these plans, created my backups (two, just in case), verified them, and then had a failed upgrade anyway—only to discover that I had no clue where to find the original operating system CD. A day later, with the missing CD located, I was able to get up and running again. My problem was an older BIOS, and the manufacturer of my computer did not have an updated BIOS.

Disk 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 500 GB hard drive, you might partition it into three logical drives:

- C: drive, which might be 200 GB
- D: drive, which might be 150 GB
- E: drive, which might be 150 GB

    The following sections detail some of the major considerations for disk partitioning:

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 16 GB of disk space for Windows 10. 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 10, 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 10 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 Windows 10 operating system files. By default, the Windows operating system files are located in a folder named `Windows`.

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 can also configure the disks during the installation of the Windows 10 operating system.

You might want to create only the first partition where Windows 10 will be installed. You can then use the Disk Management utility in Windows 10 to create any other partitions you need. The Windows 10 Disk Management utility is covered in Chapter 3, "Configuring Storage and Security."

Language and Locale

Language and locale settings determine the language the computer will use. Windows 10 supports many languages for the operating system interface and utilities.

Locale settings are for configuring the format for items such as numbers, currencies, times, and dates. For example, English for the 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 10

You can install Windows 10 either from the bootable DVD or through a network installation using files that have been copied to a network share point or USB device. You can also launch the setup.exe file from within the Windows 10 operating system to upgrade your operating system.

To start the installation, you simply restart your computer and boot to the DVD. The installation process will begin automatically. You will walk through the steps of performing a clean install of Windows 10 from the DVD in Exercise 1.1.

If you are installing Windows 10 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 10 distribution files copied to a shared folder. The following steps are used to install Windows 10 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 10 installation using either the clean install method or the upgrade method. These methods are discussed in detail in the following sections.

Performing a Clean Install of Windows 10

On any installation of Windows 10, there are three stages.

Collecting Information   During the collection phase of the installation, Windows 10 gathers the information necessary to complete the installation. This is where Windows 10 gathers your local time, location, keyboard, license agreement, installation type, and installation disk partition information.

Installing Windows   This section of the installation is where your Windows 10 files are copied to the hard disk and the installation is completed. This phase takes the longest because the files are installed.

Setting Up Windows   In this phase, you set up a username, computer name, and password; enter the product key; configure the security settings; and review the date and time. Once this is finished, your installation will be complete.

As explained earlier, you can run the installation from the optical media, from a USB, or over a network. The only difference in the installation procedure is your starting point: from your optical drive or USB or a network share. The steps in Exercise 1.1 and Exercise 1.2 assume you are using the Windows 10 DVD to install Windows 10.

Setting Up Your Computer for Hands-On Exercises

Before beginning Exercise 1.1, verify that your computer meets the requirements for installing Windows 10, as listed earlier in Table 1.3. For Exercise 1.1, it is assumed you are not currently running a previous version of Windows that will be upgraded.

The exercises in this book are based on your computer being configured in a specific manner. Your computer should have at least a 50 GB hard drive (this exceeds the basic minimums) that is configured with the minimum space requirements and partitions.

When you boot to the Windows 10 installation media, the Setup program will automatically start the Windows 10 installation. In Exercise 1.1, you will perform a clean install of Windows 10. This exercise assumes that you have access to Windows 10 Enterprise; other editions may vary slightly. You can also download an evaluation version of Windows 10 from the Microsoft website.

Also, I may list steps that you may not see or I may not list steps that you see—this is because my version of Windows may be different. For example, I am installing an MSDN Windows 10 Enterprise edition. At this time, I am not required to enter a license number during install. A normal version bought from a vendor may ask for the license during the actual install.

> **NOTE** I am loading Windows 10 Enterprise into a VMware Workstation virtual machine. Again, this may make your installation a little different than the steps listed in Exercise 1.1.

EXERCISE 1.1

Performing a Clean Install of Windows 10

1. Insert the Windows 10 DVD into a machine or virtual machine with no operating system and start the computer.

2. If you are directed to "Hit any key" to start the DVD, press Enter.

3. The first screen will ask you to enter your language, time and currency format, and keyboard or input method (see Figure 1.1). After filling in these fields, click Next.

FIGURE 1.1   Windows Setup screen

4. On the next screen, click the Install Now button (see Figure 1.2).

FIGURE 1.2   Windows install screen
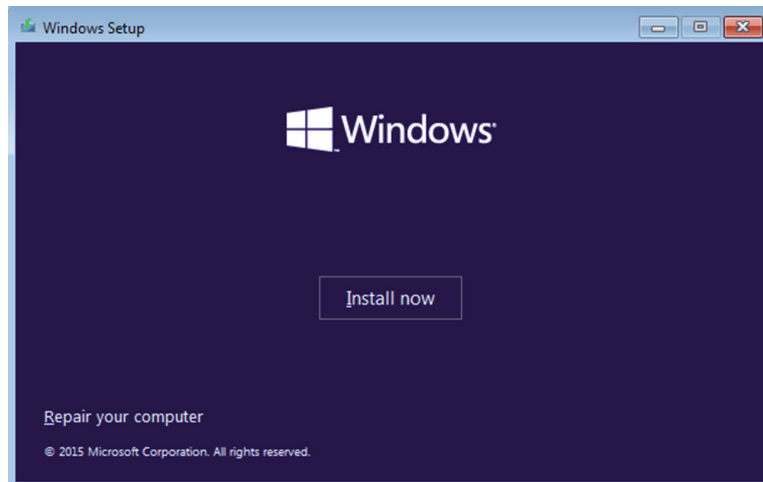
5. A message appears to tell you that the setup is starting. The licensing screen
    will be first. Read the license agreement and then check the I Accept The License
    Terms check box (see Figure 1.3). Click Next.

FIGURE 1.3   Windows license screen
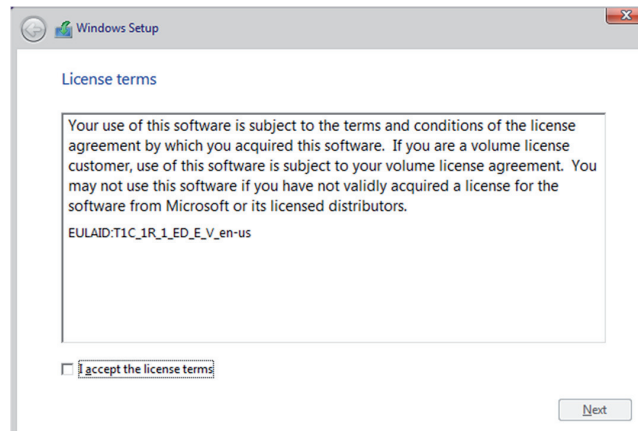
6. When asked which type of installation you want, click Custom (Advanced) as shown
    in Figure 1.4.

FIGURE 1.4 Type of install screen
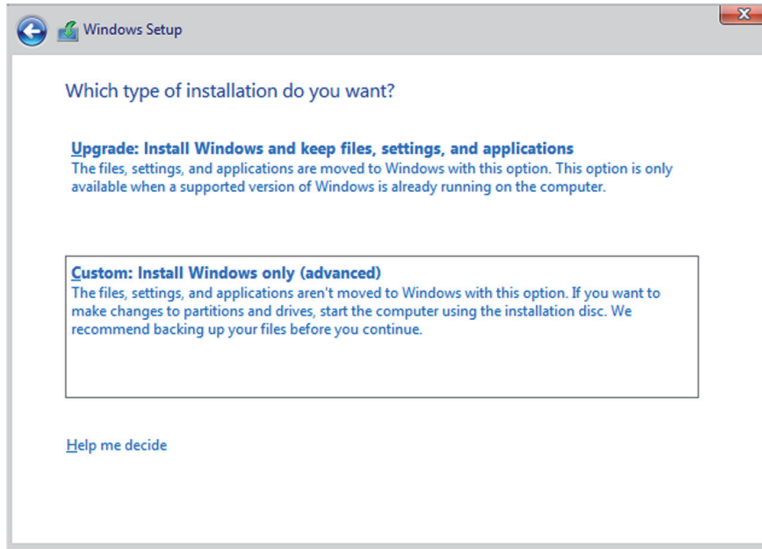
7. The next screen asks you to identify the disk to which you would like to install Windows 10. Choose an unformatted free space or a partition (partition will be erased) with at least 50 GB available. You can also click the Drive Options (Advanced) link to create and format your own partition as shown in Figure 1.5. After you choose your partition, click Next.

FIGURE 1.5 Windows disk setup screen
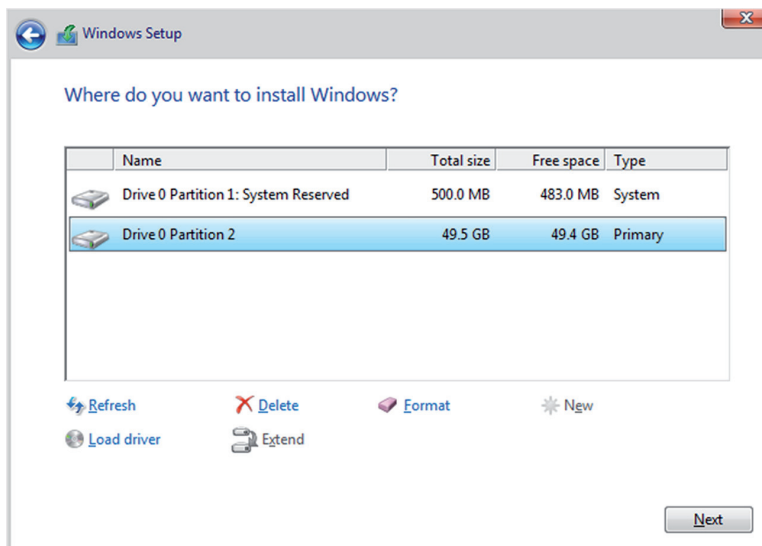
8. When your partition is set, the installation will start (as shown in Figure 1.6). You will see the progress of the installation during the entire process. When the installation is complete, the machine will reboot.

    FIGURE 1.6   Windows installation status screen
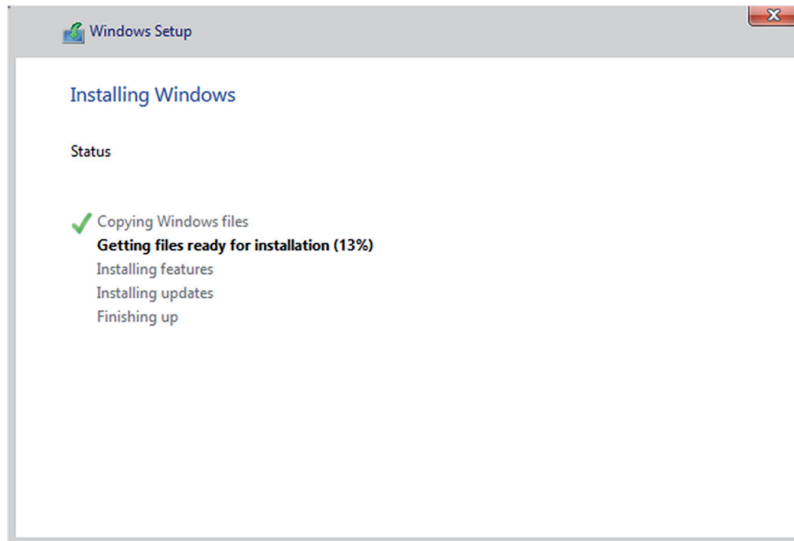
9. After the system restarts, a screen appears that asks if you want to use custom or express settings, as shown in Figure 1.7. Click the Use Express Settings button. The system will then restart.

    FIGURE 1.7   Windows express settings screen
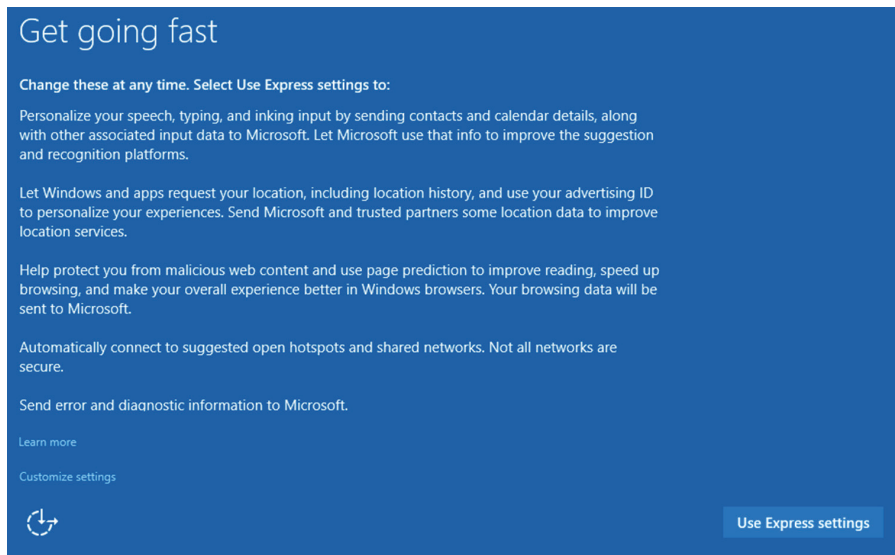
10. After the restart, a screen appears that asks you to choose how you will connect. Select Join A Domain (see Figure 1.8), and then click the Next button.

FIGURE 1.8   Choosing a domain
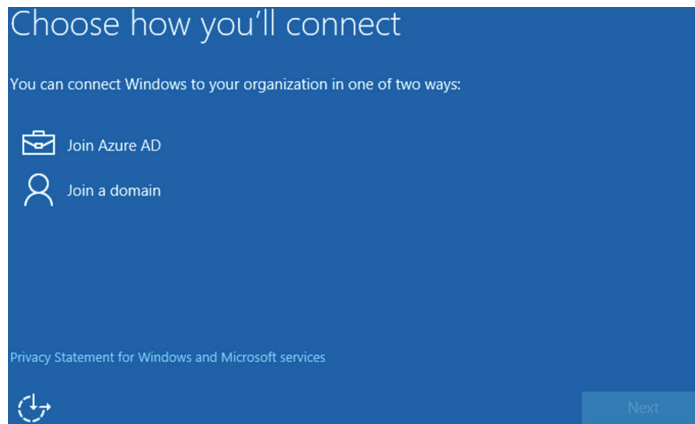
11. The next screen asks you to enter a username and password. Type in your username, password, and a password hint, as shown in Figure 1.9. Then click Next.

FIGURE 1.9   PC account screen
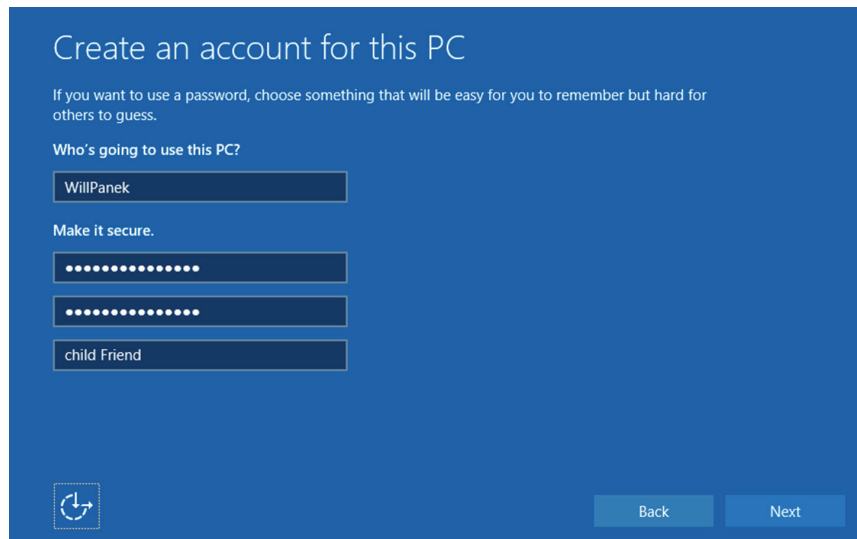
The Hi screen will appear, and the system will continue its setup. Then the system applications will be installed.

12. You will be asked if you want your system to be recognized by other systems on the network. This is a choice you can make. If you want other machines to see this Windows 10 system, choose Yes.

Once Windows 10 finishes its installation, you should see the Windows 10 desktop, as shown in Figure 1.10.

FIGURE 1.10 Windows 10 screen
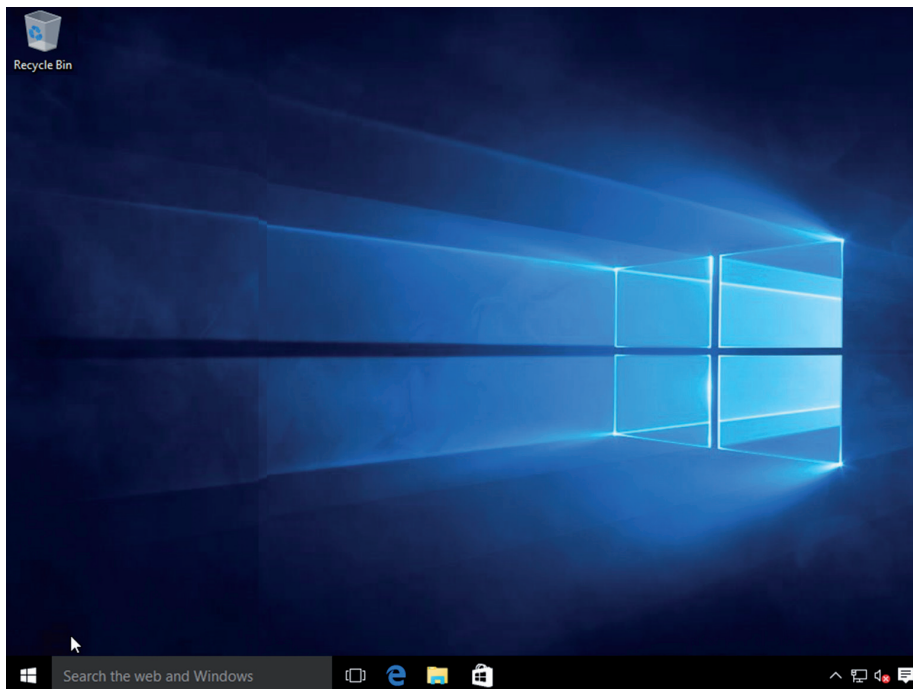
Before we talk about the Windows 10 upgrade procedure, I want to quickly explain something that you saw during the Windows 10 install. In step 10, I had you choose Join A Domain instead of Azure AD. We will explore both of the choices in greater detail, but I wanted to quickly explain why we chose one over the other.

Microsoft offers two main networks: workgroup-based or domain-based. *Workgroups* (also referred to also as peer-to-peer networks) is when you just connect your computers together directly to each other. A perfect example for most of us is what you do in your home network. Most home users connect their machines together without the use of a main server.

Corporations normally do things a bit differently than that. *Domains* are networks that are controlled by servers called domain controllers. Domain controllers are Windows servers that have a copy of a database called Active Directory (AD). Recently Microsoft took domain-based networks a step further by allowing companies to set up a cloud-based version of an Active Directory domain (Azure AD). This means that companies no longer need to maintain and manage their own domain controllers. Since most people don't have a cloud-based version of Azure AD, I had you choose the option Join A Domain so that we could finish the Windows 10 install.

We will go over all of these options in greater detail throughout this book, but I wanted to introduce you to these two Windows 10 options.

Performing an Upgrade to Windows 10

This section describes how to perform an upgrade to Windows 10 from Windows 8.1. Similar to a clean install, you can run the installation from the installation DVD, from a USB, or over a network. The only difference in the installation procedure is your starting point: from your optical or USB drive or from a network share. For the steps in the following sections, it is assumed that you are using the Windows 10 DVD to install the Windows 10 operating system.

Upgrading a Windows 7 or Windows 8.1 system to Windows 10 will save you a lot of time and trouble. Because we are upgrading the system, all of the user's data and applications will remain installed and most likely still work the exact same way. Sometimes when we upgrade a system, we run into problems with applications. But many times that is caused by a driver or a needed software update that will most likely solve the issue.

The three main steps in the Windows 10 upgrade process are very similar to the ones for a clean install. The three steps of upgrading to Windows 10 are as follows:

1. Collecting information

2. Installing Windows

3. Setting up Windows

In Exercise 1.2, you will go through the process of installing Windows 10 by upgrading Windows 8.1. As you can see in Figure 1.11, I have a Windows 8.1 Enterprise system that I will update to Windows 10 Enterprise.

FIGURE 1.11   Windows 8.1
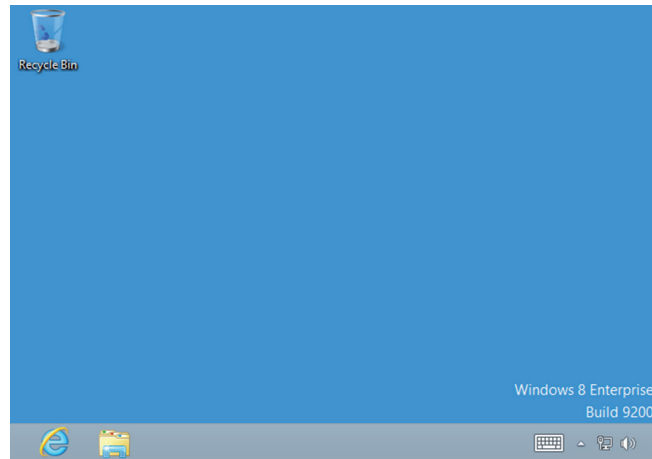
EXERCISE 1.2

Upgrading Windows 8.1 to Windows 10

1. Insert the Windows 10 DVD. (We are upgrading Windows 8.1 Enterprise to Windows 10 Enterprise.)

2. If Autorun does not start, navigate to the DVD drive and click setup.exe. Once the setup starts (via either setup.exe or Autorun), click Run Setup.exe as shown in Figure 1.12.

FIGURE 1.12   DVD setup screen
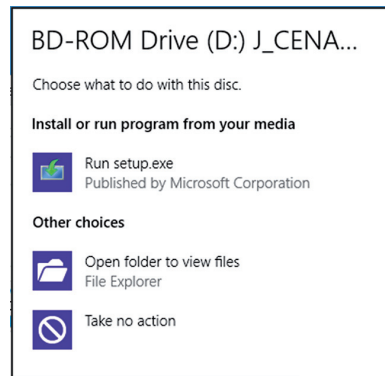
3. If a pop-up box appears for User Account Control, click the Yes button (see Figure 1.13).

F I G U R E   1 . 1 3   User Account Control screen
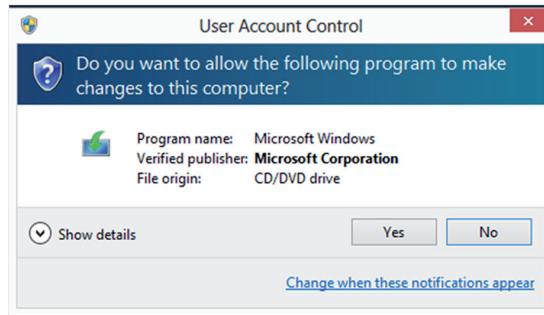
You should then see a message appear stating that Windows is preparing the system, as shown in Figure 1.14.

F I G U R E   1 . 1 4   Preparing screen
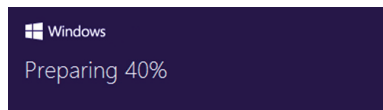
4. You may be prompted to Get Important Updates. You can choose to either download the updates or not do them at this time. Make a choice and click the Next button. (During my installation, I decided to download the updates.)

5. The Microsoft Windows 10 license terms appear. Read the terms and then click Accept. (The installation will not allow you to continue until you click Accept.)

6. At the Ready To Install screen (shown in Figure 1.15), you can change what files and/or apps you want to keep by clicking the Change What To Keep link. Once you're ready, click the Install button.

FIGURE 1.15   Ready To Install screen
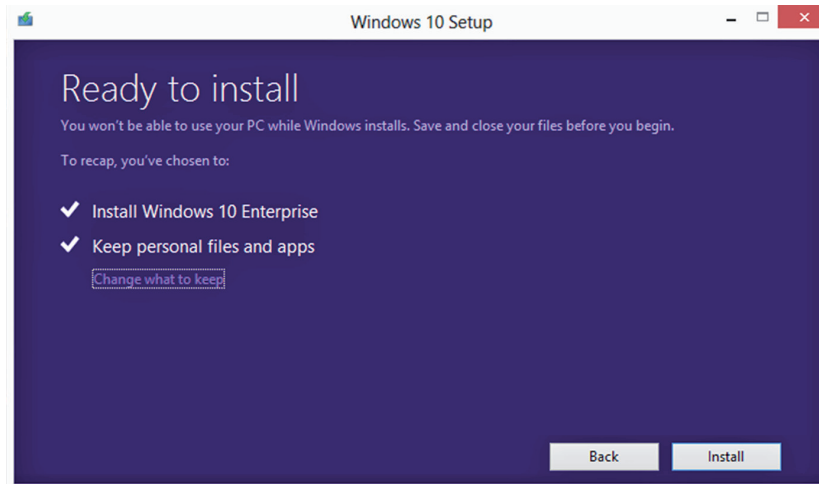
7. Windows 10 will begin to install (as shown in Figure 1.16). Your computer may restart multiple times. This is normal. As the upgrade status screen states, "Sit back and relax."

FIGURE 1.16   Installing Status screen
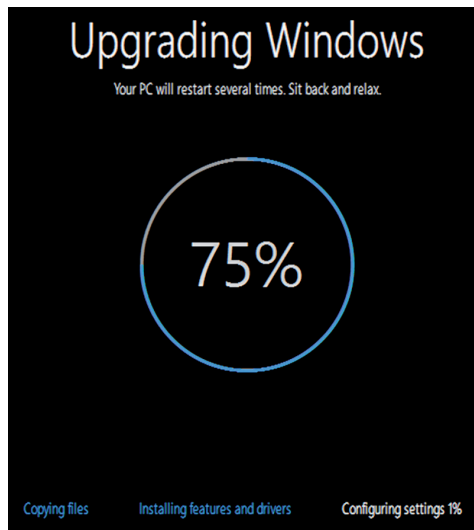
8. After the upgrade has completed, a welcome screen will be displayed, similar to the one shown in Figure 1.17. Click Next.

   FIGURE 1.17 Welcome screen
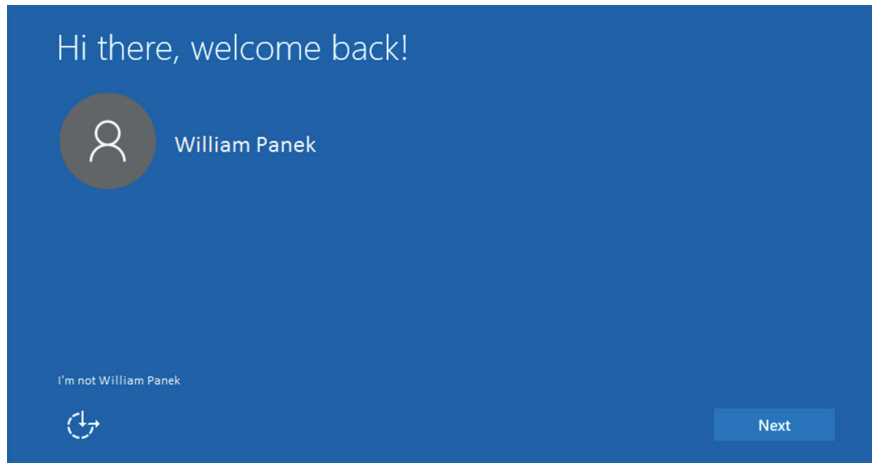
9. At the Get Going Fast screen, click the Use Express Settings button.

10. At the New Apps screen, just click Next.

    And that's it—Windows 10 is installed (see Figure 1.18). Congrats.

    FIGURE 1.18 Windows 10 screen
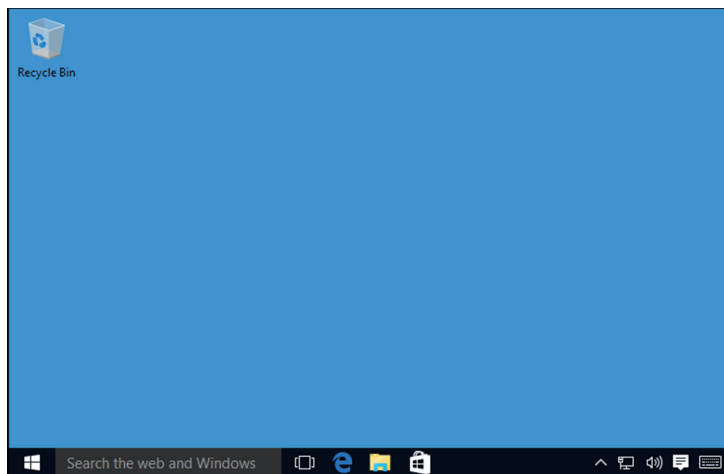
Troubleshooting Installation Problems

The Windows 10 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 will occur.

Identifying Common Installation Problems

As most of you are aware, installations sometimes do get errors. You might encounter some of the following installation errors:

Media Errors Media errors are caused by defective or damaged 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 10 needs at least 16 GB for the 32-bit OS and 20 GB for the 64-bit OS to execute properly. If the Setup program cannot verify that this space exists, the program will not let you continue.

Not Enough Memory Make sure your computer has the minimum amount of memory required by Windows 10 (1 GB for 32-bit or 2 GB for 64-bit). Having insufficient memory may cause the installation to fail or blue-screen errors to occur after installation.

Not Enough Processing Power Make sure your computer has the minimum processing power required by Windows 10 (1 GHz or faster processor or SoC). 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 10 may not recognize the hardware or the device may not work properly.

Hardware with No Driver Support Windows 10 will not recognize hardware without driver support.

Hardware That Is Not Configured Properly If your hardware is Plug and Play (PnP) compatible, Windows 10 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 you have not typed in an incorrect key (check your Windows 10 installation folder or your computer case for this key).

Failure to Access TCP/IP Network Resources If you install Windows 10 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 10 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 for Windows 10 from the manufacturer and then specify the driver location by selecting the Load Driver option during partition selection.

Troubleshooting with Installation Log Files

When you install Windows 10, 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 10 Setup logs to determine whether there were any problems with your Windows 10 installation.

EXERCISE 1.3

Troubleshooting Failed Installations with Setup Logs

1. Select Start ➢ Computer.

2. Double-click Local Disk (C:).

3. Double-click Windows.

4. In the `Windows` folder, double-click the `Setupact.log` file to view your action log in Notepad. When you are finished viewing this file, close Notepad.

5. Double-click the `Setuperr.log` 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.

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 (USMT)*. USMT can help you migrate user profiles, configure folder locations for uploads and downloads of user data, and configure profile versions: local, roaming, and mandatory.

User State Migration Tool

You can download a utility called USMT that is used by administrators to migrate large numbers of users over automated deployments. USMT for Windows 10 is now part of the Windows Assessment and Deployment Kit (ADK). USMT is similar to Windows Easy Transfer, with the following differences:

- USMT is more configurable and can use XML files to specify which files and settings are transferred.

- USMT is scriptable and uses command-line utilities to save and restore user files and settings.

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. ScanState is used on the machine you are migrating from.

- `Loadstate.exe` then deposits the information that is collected to a computer running a fresh copy of Windows 10. The `Config.xml` file can be used to help exclude files and settings during the LoadState process. The LoadState command is used to bring the user data that was collected from the ScanState utility over to the new Windows 10 system.

The following information is migrated:

- From each user:
    - Documents
    - Video
    - Music
    - 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 filename extensions, including .doc, .dot, .rtf, .txt, .wps, .wri, .xls, .csv, .wks, .ppt, .pps, .pot, .pst, and more
- Access control lists (ACLs)

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

A decision point that exists while using USMT is to determine if you want to perform a side-by-side installation or a wipe-and-load installation.

Side-by-Side Installation   A side-by-side installation means that you have the new computer and the old computer. You use ScanState to collect the user's data. You then store that data on an intermediate store. After the installation of Windows 10 on a new machine, you use LoadState to move the data from the intermediate store to the new computer.

Wipe-and-Load Installation   A wipe-and-load installation means that you have the old computer only. You will install Windows 10 on the same machine as the previous operating system. You use ScanState to collect the user's data. You then store that data on an intermediate store. After the installation of Windows 10 on the machine, you use LoadState to move the data from the intermediate store to the old computer.

USMT is downloadable software from Microsoft's website. In its simplest form, you use 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 10 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 USMT, you can create a script that can be run manually or can be used as an automated process at a scheduled time. Table 1.5 defines the options for the Scanstate .exe and Loadstate.exe commands.

TABLE 1.5   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

Option	Description
/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 0–13, with 0 being the least verbose

Migrating Profiles

Even an operating system that you install has a user profile. User profiles are created when a user logs into a system for the first time. The user profile is a group of settings that make the computer look and work the way you want it to. It contains your settings for desktop backgrounds, screen savers, pointer preferences, sound settings, and other features. Each user account has at least one user profile associated with it. To view the user profiles on a system, you view the Advanced tab of the System Properties (see Figure 1.19).

F I G U R E 1.19   User Profiles Settings button
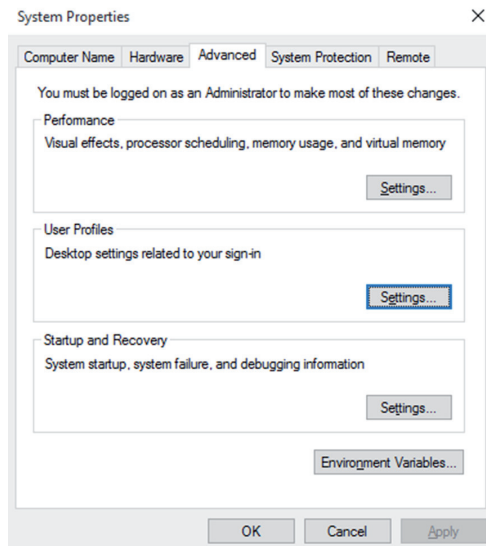
User profiles ensure that your personal preferences are used whenever you log on to Windows. User profiles are not user accounts; rather, they specify how the user account's desktop and settings are configured.

There are different types of user accounts: local, roaming, and mandatory. *Local profiles* are used when you log into a local system or a network system that doesn't use network profiles.

A local profile can be saved to a network location, and then the user's network account can point to that network profile location. This is referred to as a *roaming profile*. Roaming profiles are just local profiles saved to a network location. No matter which system you log into on your network, your desktop and user profile will be the same. The profile follows the user.

To copy a local profile to the network, click the user's profile and then click the Copy To button (see Figure 1.20). Place the user's profile on a network share, and then in the Active Directory account properties for that user, point to the network profile (for example, *Server**ShareName**UserName*). You have now created a roaming profile.

FIGURE 1.20 Local user profiles
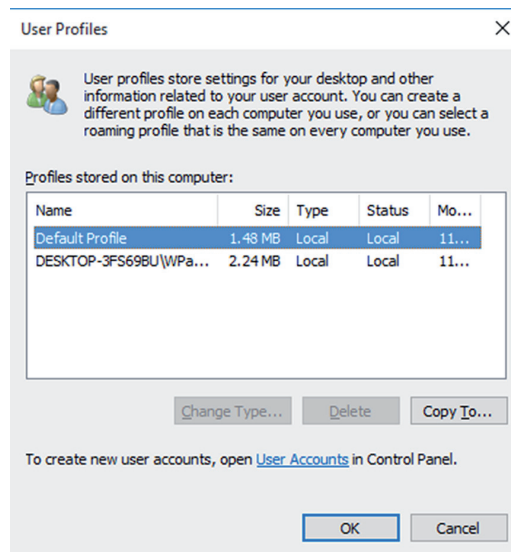
To change a roaming profile to a *mandatory profile* (a profile that is mandatory), just change the name of the user profile with the extension of .man. So, for example, if Will Panek's roaming profile is called NTuser.dat, you would change it to NTuser.man. By adding the .man extension, you have made the profile mandatory. Now the user would have to use this profile when he or she logs into the network.

Supporting Multiple-Boot Options

You may want to install Windows 10 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

dual-boot–supported operating system on your computer prior to the Windows 10 installation, you didn't upgrade from that operating system, and you installed Windows 10 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 should dual-boot. For example, you might configure one computer to dual-boot with Windows 7, Windows 8.1, and Windows 10.

Here are some keys to successful dual-boot configurations:

- Make sure you have plenty of disk space.

- Windows 10 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 Windows 7 and Windows 10, Windows 7 must be installed first. If you install Windows 10 first, you cannot install Windows 7 without ruining your Windows 10 configuration.

- Do not install Windows 10 on a compressed volume unless the volume was compressed using NTFS compression.

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 the [Windows] key + R and then entering **cmd**.

3. Type **cmd.exe** in the Search Programs And Files box and press Enter.

Once the command-prompt window is open, type bcdedit to launch the **bcdedit** utility. You can also type **bcdedit/?** to see all the different bcdedit commands. A few bcdedit commands may be needed when dual-booting a machine. Table 1.6 shows some of the bcdedit commands that may be needed when dual-booting.

TABLE 1.6   Bcdedit commands for dual-booting

Command	Explanation
/createstore	Creates a new empty boot configuration data store
/default	Allows you to specify which operating system will start when the time-out expires
/deletevalue	Allows you to delete a specified element from a boot entry

TABLE 1.6   `Bcdedit` commands for dual-booting *(continued)*

Command	Explanation
`/displayorder`	Shows the display order that the boot manager uses when showing the display order to the user
`/export`	Allows you to export the contents of the system store into a file
`/import`	Restores the system store by using the data file previously generated by using the `/export` option
`/set`	Allows you to set an entry option value
`/store`	Specifies the store to be used
`/timeout`	Specifies the amount of time used before the system boots into the default operating system

Using Windows Activation

Windows Activation is Microsoft's way of reducing software piracy. Unless you have a corporate license for Windows 10, you will need to perform postinstallation activation. This can be done online or through a telephone call. Windows 10 will attempt automatic activation three days after you log on to it for the first time. There is a 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 10 is activated. When the grace period runs out, the Windows Activation Wizard will automatically start (see Figure 1.21); it will walk you through the activation process. You may need to click the Change Product Key button and put in the license number that came with your Windows 10 copy.

Using Windows Update

Windows Update is a utility that connects to the Microsoft website and checks to ensure that you have the most up-to-date versions of Microsoft products.

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

- Critical updates
- Service packs
- Drivers

FIGURE 1.21   The Windows Activation Wizard screen
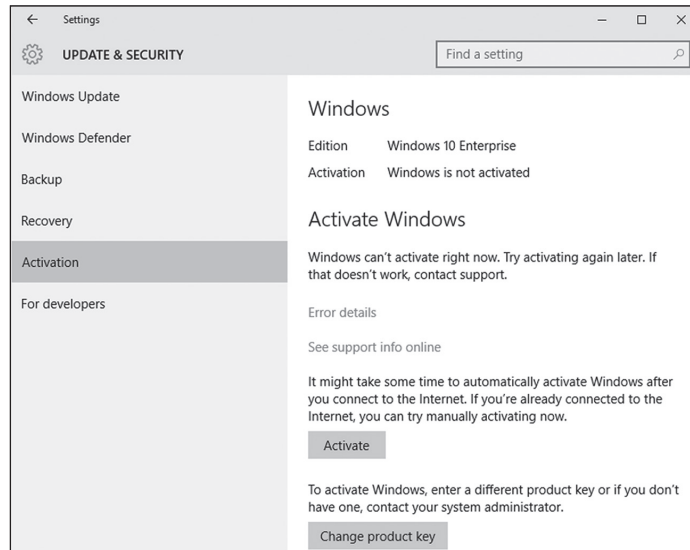
Follow these steps to configure Windows Update:

1. Select Start ➢ Control Panel.

- From Windows Icons View, select Windows Update.
- From Windows Category View, select System And Security ➢ Windows Update.

2. Configure the options you want to use for Windows Update by clicking the Advanced Options link. The options you can access from Windows Update include the following:

- Choose how updates are installed
- Give me updates for other Microsoft products
- Defer Upgrades
- View Update History
- Choose how updates are delivered
- Get Insider Builds

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 1.22 shows the Check for Updates button.

FIGURE 1.22   Check for updates button
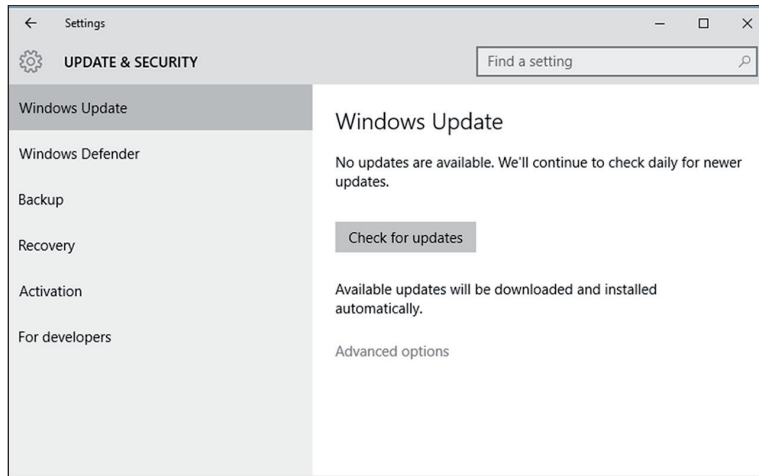
There are two ways a user can receive updates: directly from Microsoft or using Microsoft Windows Server Update Service (WSUS). WSUS runs on a Windows server, and that server goes out to the Microsoft website and downloads the updates for your Windows clients. This allows client machines to receive their updates from a local server.

One advantage to using WSUS is that administrators can approve the updates before they get deployed to the client machines. Another advantage is that your clients only need to download updates locally, without using your Internet bandwidth.

> WSUS is discussed in detail in *MCSA: Windows Server 2012 R2 Complete Study Guide* by William Panek (Sybex, 2015).

Using Command-Line Options

Command-line options are becoming more and more popular among administrators and users. Windows Update has a few command-line options that can be used to help configure and maintain it. First, to start Windows Update from a command prompt, you can type **wuapp.exe**. Another command-line option that works with Windows Update is called Windows Update Automatic Update Client (`wuauclt.exe`), which offers the following options:

Detectnow   When working with WSUS, waiting for detection to start can become very time-consuming. So Microsoft has added an option to allow you to initiate the process of

detecting available updates right away. To run the `detectnow` option, type the following command at the command prompt: **`wuauclt.exe /detectnow`**.

`Reportnow`   This command allows you to send all queued reporting events to the server asynchronously. To execute this command, type **`wuauclt.exe /reportnow`** at the command prompt.

`Resetauthorization`   WSUS uses a cookie on Windows 10 client computers to store different types of information. By default, an hour after the cookie is created, it expires. If you need the cookie to expire now, you can use the `resetauthorization` option along with the `detectnow` option. Using these options will expire the cookie, initiate detection, and have WSUS update computer group membership. To execute this command, type **`wuauclt.exe /resetauthorization /detectnow`** at the command prompt.

Installing Windows Service Packs

Service packs are updates to the Windows 10 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

`http://windows.microsoft.com/en-US/windows/downloads/service-packs`

You can also receive service packs via Windows Update, or you can pay for a copy of a service pack to be mailed to you on disk. Before you install a service pack, you should read the release notes that are provided on the Microsoft website.

Summary

This chapter started with a discussion of the features included with Windows 10. We also took a look at the difference between 64-bit and 32-bit operating systems and showed some of the advantages that 64-bit entails, such as greater RAM and processor speed.

Then you learned about installing Windows 10. Installation is an easy process, but you must first make sure the machine is compatible with the Windows 10 operating system.

There are two main ways to install Windows 10: upgrade or clean install. You can upgrade a Windows 7 or Windows 8 machine to Windows 10. You can migrate the user's data and information from a Windows XP machine, but there is no direct upgrade option.

After the Windows 10 installation is complete, you'll want to make sure all updates and service packs are installed. You can use Windows Update to complete that task.

Video Resources

There are videos available for the following exercises:

   1.1

   1.2

   You can access the videos at www.wiley.com/go/sybextestprep on the Other Study Tools tab.

Exam Essentials

Understand the Windows 10 hardware requirements.   The minimum hardware requirements to run Windows 10 properly are 1 gigahertz (GHz) or faster processor or SoC, 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit of RAM, 16 GB for 32-bit OS 20 GB for 64-bit OS of hard drive space, DirectX 9 or later with WDDM 1.0 video driver, and a DVD-R/W drive or compatible network interface card.

Understand the Hardware Compatibility List.   The Hardware Compatibility List (HCL) is an extensive list of computers and peripheral hardware devices that have been tested with the Windows 10 operating system. The hardware and supported drivers on the HCL have been put through rigorous tests to ensure their compatibility with Windows 10. Microsoft guarantees that the items on the list meet the requirements for Windows 10 and do not have any incompatibilities that could affect the stability of the operating system.

Understand how to complete a clean install.   If your machine meets the minimum hardware requirements, you can install Windows 10. There are a few different ways to install Windows 10 onto a computer. You can use the installation disk or USB, install it over a network, or install it from an image (see Chapter 2, "Automated Windows 10 Deployments," for more details on imaging).

Understand how to complete an upgrade.   You can't upgrade a Windows Vista machine to Windows 10. To complete an upgrade on a Windows 7 or Windows 8 machine, insert the Windows 10 DVD into the Windows machine or connect to the Windows 10 files over the network and complete an upgrade on the computer.

You can't upgrade a Windows XP machine directly to Windows 10. If the machine is running Windows XP, you have to use a migration tool to migrate all the user data from Windows XP to a Windows 10 machine.

Understand how to migrate a user to Windows 10.   If you can't perform an upgrade on the computer, you can choose to migrate the user's files and settings from an existing installation. In this case, you can use the User State Migration Tool (USMT).

Review Questions

1. You are the administrator in charge of a computer that runs both Windows 7 and Windows 10. Windows 10 is installed on a different partition from Windows 7. You have to make sure that the computer always starts Windows 7 by default. What action should you perform?

    A. Run `Bcdedit.exe` and the `/default` parameter.

    B. Run `Bcdedit.exe` and the `/bootcd` parameter.

    C. Create a `Boot.ini` file in the root of the Windows 10 partition.

    D. Create a `Boot.ini` file in the root of the Windows 7 partition.

2. You are the administrator for a Windows 10 computer. You have decided to use Windows Update, but you want to be able to change the settings manually. What should you do?

    A. Log on to Windows 10 as a member of the Administrators group.

    B. From the local Group Policy, modify the Windows Update settings.

    C. Right-click Windows Update and select Run As Administrator.

    D. Right-click the command prompt, select Run As Administrator, and then run `Wuapp.exe`.

3. You have two computers: System1 and System2. System1 runs the Windows 7 operating system, and System2 runs Windows 10. You need to migrate the profiles and user files from System1 to System2. You need to identify how much space is required to complete the migration. What action should you perform?

    A. On System1, run `Loadstate c:\store /nocompress`.

    B. On System2, run `Loadstate \\system1\store /nocompress`.

    C. On System1, run `Scanstate c:\store /nocompress /p`.

    D. On System2, run `Scanstate \\system1\store /nocompress /p`.

4. You are the IT manager for a medium-size organization. Your organization is looking at upgrading its Windows XP machines to Windows 10. The managers have heard of a new feature that allows you to connect a device to the machine and then the Windows 10 operating system shows a graphic of the device for use. Which Windows 10 feature are they referring to?

    A. Device Manager

    B. Device Stage

    C. Staging Manager

    D. Add/Remove Hardware

5. You are the IT manager for your organization. The organization is looking at upgrading all of its machines from Windows XP to Windows 10. Many of the managers are concerned that their Windows XP applications won't be compatible with Windows 10. Which

Windows 10 feature can you use to assure the managers that all of their Windows XP applications will continue to work?

A.   Windows XP Compatibility Checker

B.   Windows XP Application Center

C.   Windows Hyper-V client

D.   Windows XP Application Upgrade tool

6.   You are the network administrator for a midsize company that needs to convert all of its Windows XP machines to Windows 10. How can the IT department put Windows 10 on all the Windows XP machines without losing any of the users' information?

A.   Upgrade all the Windows XP machines to Windows 10.

B.   Format all the XP machines and do a clean install of Windows 10.

C.   Use a migration tool to migrate all the users' data and then load a clean copy of Windows 10.

D.   Do nothing. The Windows XP machines can't be upgraded without losing all the users' data.

7.   You are the IT administrator for a large computer-training company that uses laptops for all its employees. Currently the users have to connect to the wireless network through the wireless network adapter. Windows 10 now includes this built in as which feature?

A.   Available Network Finder (ANF)

B.   View Networks (VN)

C.   Network Availability Viewer (NAV)

D.   View Available Networks (VAN)

8.   You are the network administrator for a midsize company. One of the managers has come into your office and asked you about setting up a network in his house. He wants to use Windows 10. What feature allows him to set up a home network using Windows 10?

A.   Home Networking

B.   HomeGroup

C.   Quick Connect

D.   Networking Groups

9.   Which new Windows 10 feature allows you to quickly access files that you have been working on?

A.   Quick Connect

B.   Jump Lists

C.   File Finder

D.   Quick File Access

10. You are the IT manager for a pharmaceutical company. The company wants to create a medication dispenser that can be used on the floors of hospital units. The dispensers have to work through touch-screen technology. Which Windows 10 feature provides built-in touch-screen technology?

A. Windows Touch Screen

B. Windows Pure Touch

C. Windows Touch

D. Windows Pure Screen

Chapter

2

Automated Windows 10 Deployments

MICROSOFT EXAM OBJECTIVES COVERED
IN THIS CHAPTER:

✓ **Configure Hyper-V.**

   ▪ This objective may include but is not limited to the following
   subobjectives: Create and configure virtual machines
   including integration services, create and manage check-
   points, create and configure virtual switches, create and
   configure virtual disks, move a virtual machine's storage.

Installing Windows 10 is quick and easy, but as an IT manager or IT professional, you may have to install hundreds of copies of Windows 10. It is not a good practice to install them one at a time. It's important to understand how to automate a Windows 10 deployment for the Windows 10 (70-697) exam, but you'll also use automated deployments in a corporate environment. Many companies use third-party tools to create and deploy Windows 10 machines, but there are other ways.

You can automate the installation of Windows 10 in several ways. You can install Windows 10 by using an unattended installation, by using Windows Deployment Services (WDS) to remotely deploy unattended installations (which requires a Windows Server 2012 R2 machine), by using Hyper-V, 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 to provide answers to the questions that are normally asked during the installation process. After you've installed Windows 10, you can also automate the installation of applications by using Windows Installer packages.

This chapter also includes the following topics:

- An overview of the automated deployment options
- How to access the deployment tools available for Windows 10 and the use of unattended installation
- WDS
- How the System Preparation Tool (along with Image Capture Wizard) is used to create disk images for automated installation
- How to use Windows System Image Manager (SIM) to create unattended answer files

I will also talk about how to set up and configure Hyper-V. Windows 10 can be loaded onto a Windows Server 2012 R2 Hyper-V server, or Windows 10 can also act as a Hyper-V server.

Understanding Automated Deployment Options

If you need to install Windows 10 on multiple computers, you could manually install the operating system on each computer, as described in Chapter 1, "Installing Windows 10." 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 on which to install Windows 10.

Windows 10 comes with several utilities that can be used for deploying and automating the Windows 10 installation. With access to multiple utilities with different functionality, administrators have increased flexibility in determining how to best deploy Windows 10 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 this chapter. The options for automated deployment of Windows 10 are as follows:

- Microsoft Deployment Toolkit (MDT) 2013 Update 1
- Unattended installation, or unattended setup, which uses `Setup.exe`
- WDS, which requires Windows Server 2012 R2 for deployment
- Windows 10 Assessment and Deployment Kit (ADK), which also includes the System Preparation Tool (`Sysprep.exe`), used to create images or clones
- Windows Imaging and Configuration Designer (Windows ICD)

Table 2.3, later in the chapter, summarizes the features and requirements of each installation deployment option.

> **NOTE**
>
> Another option that you have to deploy Windows 10 is through System Center Configuration Manager (SCCM). Since SCCM is its own application, it is beyond the scope of this book. You can learn more about SCCM on the Microsoft website at `http://www.microsoft.com`.

An Overview of the Microsoft Deployment Toolkit 2013

Microsoft released a deployment assistance toolset called the *Microsoft Deployment Toolkit (MDT) 2013*. It is used to automate desktop and server deployment. MDT provides an administrator with the following benefits:

- Administrative tools that allow for the deployment of desktops and servers through the use of a common console (see Figure 2.1)
- Quicker deployments and the capabilities of having standardized desktop and server images and security
- Zero-touch deployments of Windows 10, Windows Server 2012 and 2012 R2, Windows Server 2008, Windows Server 2008 R2, and Windows 7 and 8

FIGURE 2.1   MDT console
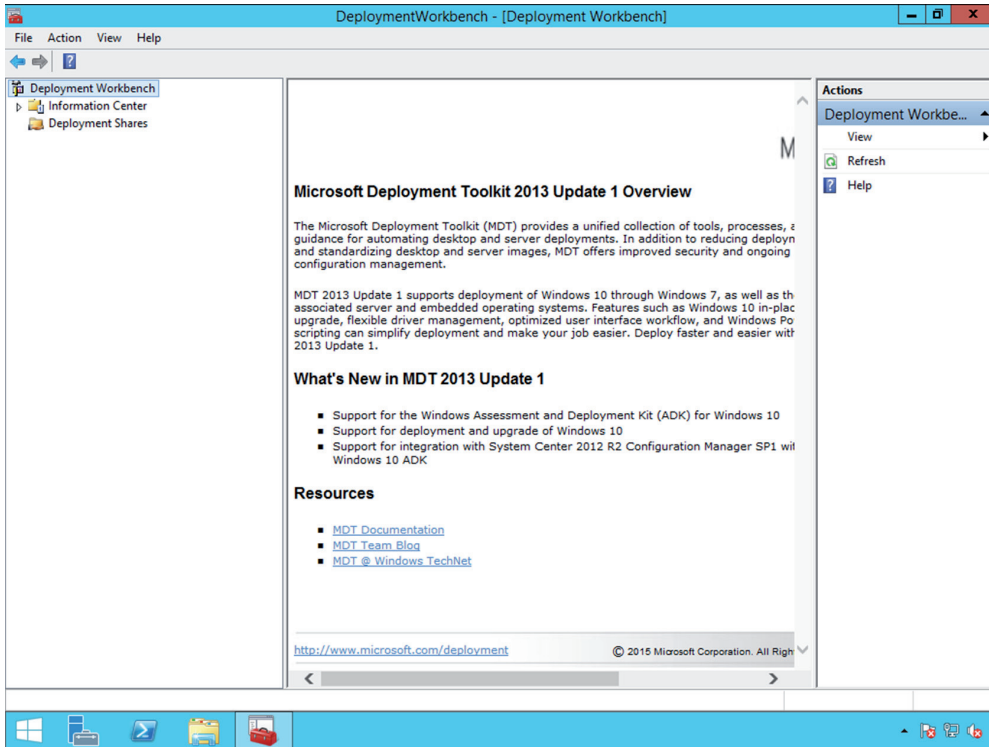
To install the MDT 2013 package onto your computer (regardless of the operating system being deployed), you must first meet the minimum requirements of MDT. These components need to be installed only on the computer where MDT 2013 is being installed:

- You can install MDT 2013 on any of the following operating systems: Windows 10, Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2.

- The Windows Assessment and Deployment Kit (ADK) for Windows 10 is required for all deployment scenarios.

- System Center 2012 R2 Configuration Manager Service Pack 1 with the Windows ADK for Windows 10 is required for zero-touch installation (ZTI) and user-driven installation (UDI) scenarios.

- If you are using ZTI and/or UDI, you are allowed to add the MDT SQL database to any version of System Center Configuration Manager with SQL technology; if you are using LTI, you must use a separately licensed SQL Server product to host your MDT SQL database.

> **NOTE** You can install MDT 2013 without installing Windows (ADK) first, but you will not be able to use the package fully until Windows (ADK) is installed.

In Exercise 2.1, you will download and install MDT 2013. You can install MDT 2013 on the Windows 10 operating system machine that you installed in Chapter 1. If you decide to install the MDT 2013 onto a server or production machine, I recommend that you perform a full backup before completing Exercise 2.1. Installing MDT 2013 will replace any previous version of MDT that the machine may currently be using.

EXERCISE 2.1

Downloading and Installing MDT 2013

To download and install MDT 2013, follow these steps:

1. Download the MDT 2013 Update 1 utility from the Microsoft website (`https://www .microsoft.com/en-us/download/details.aspx?id=48595`).

2. Click the Download button.

3. You get a screen asking you to "Choose the download you want." Choose the x64 or x86 version. Click Next.

4. A message box may appear asking if you want to run or save the MDT. I clicked the down arrow next to Save and saved the files into the downloads directory.

5. Double-click `MicrosoftDeploymentToolkit_xxx.exe` to start the installation.

6. At the Welcome screen, click Next as shown in Figure 2.2.

FIGURE 2.2 MDT Setup Wizard Welcome screen
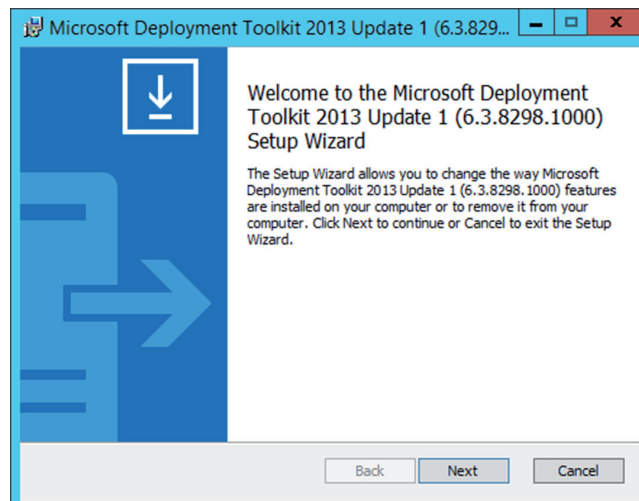
7. At the License screen, click the I Accept The Terms In The License Agreement button and click Next.

8. At the Custom Setup screen, click the down arrow next to Microsoft Deployment Toolkit and choose Entire Feature Will Be Installed On Local Hard Drive. Click Next as shown in Figure 2.3.

FIGURE 2.3   MDT Custom Setup screen
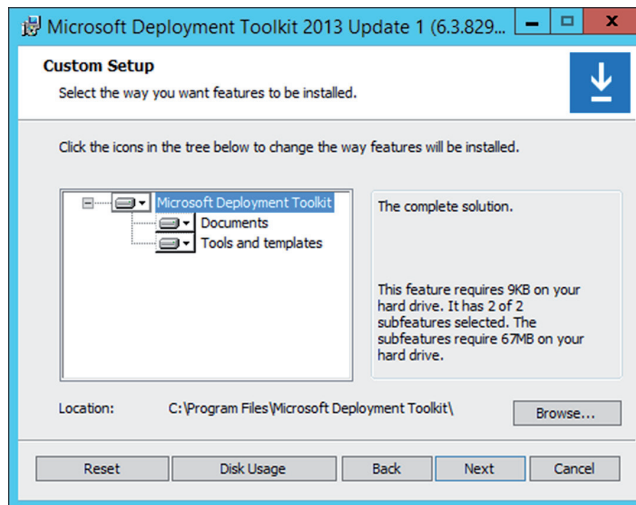
9. At the Customer Experience Improvement Program screen, choose if you want to participate or not and choose Next.

10. At the Ready To Install screen, click the Install button.

11. If a User Account Control dialog box appears, click the Yes button.

12. When the installation completes, click the Finish button.

Now that you have installed MDT 2013, you are going to configure the package. In Exercise 2.2, you will configure MDT 2013 and set up a distribution share and database. I am creating the MDT 2013 on a Windows Server 2012 R2 so that we can distribute Windows 10. Make sure the Windows Assessment and Deployment Kit (ADK) for Windows 10 is installed, because it is required for all deployment scenarios.

Configuring MDT 2013

To configure MDT 2013, follow these steps:

1. Create a shared folder on your network called `Distribution`, and give the Everyone group full control to the folder for this exercise.

2. Open the MDT workbench by choosing Start ➢ down arrow ➢ Microsoft Development Toolkit ➢ Deployment Workbench.

3. If the User Account Control box appears, click Yes.

4. In the left pane, click Deployment Shares, and then right-click the deployment shares and choose New Deployment Share.

5. The New Deployment Share Wizard begins (as shown in Figure 2.4). On the first screen, you will choose the directory where the deployments will be stored. Click the Browse button and choose the Distribution share that you created in step 1. Then click Next.

FIGURE 2.4   New Deployment Share Wizard screen
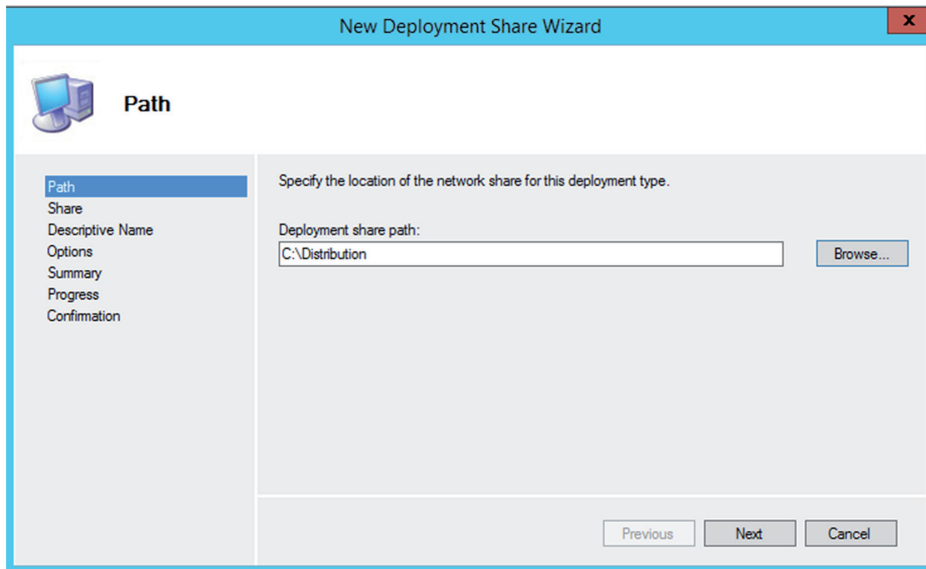
6. On the Share Name screen, accept the default, Distribution. Click Next.

7. On the Descriptive Name screen, accept the default description name (as shown in Figure 2.5) and click Next.

FIGURE 2.5 Descriptive Name screen
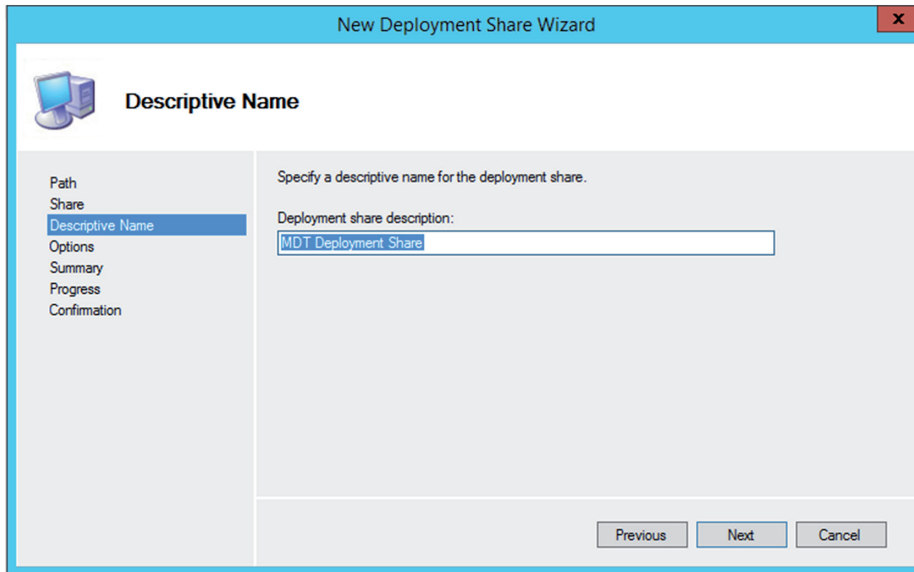
8. On the Options screen, make sure all check boxes are checked, as shown in Figure 2.6.

FIGURE 2.6 Options screen
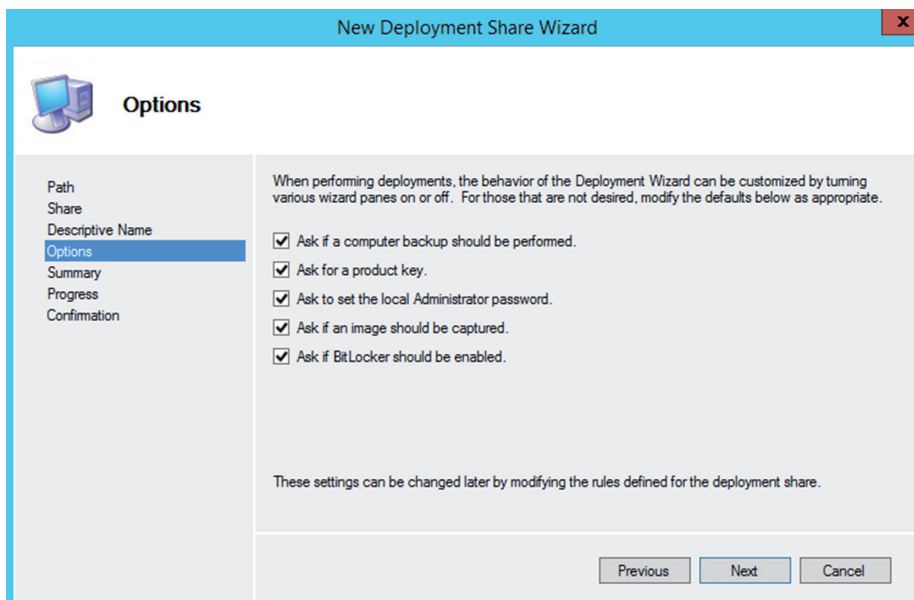
9. On the Summary screen, look over the options and click the Next button.

10. The installation Progress screen will show you how the installation is performing. When the installation is complete, click the Finish button.

    The new deployment share is set up and ready to start deploying. Now an operating system needs to be set up in the MDT 2013 for deployment.

11. Close the MDT workbench.

Now that you have seen how to install the MDT 2013 utility, let's take a look at some other ways to automatically install Windows 10.

An Overview of Unattended Installation

Unattended installation is a practical method of automating deployments when you have a large number of clients to install and the computers require different hardware and software configurations. Unattended installations allow you to create customized installations that are specific to your environment. Custom installations can support custom hardware and software installations.

Unattended installations utilize an answer file called `Autounattend.xml` to provide configuration information during the installation process. Think about the Windows 10 installation from the previous chapter. You are asked for your locale, type of installation, and so on. The answer file allows these questions to be answered without user interaction. In addition to providing standard Windows 10 configuration information, the answer file can provide installation instructions for applications, additional language support, service packs, and device drivers.

With an unattended installation, you can use a distribution share to install Windows 10 on the target computers. You can also use a Windows 10 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 10 is in XML format, all custom configuration information can be contained within the `Autounattend.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 10 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, it should contain the Windows 10 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 2.7 illustrates the unattended installation process.

FIGURE 2.7 Unattended installation with distribution share and a target computer

Distribution Share

Stores:
Windows 10 Image File
Answer File (Unattend.xml)

Target

Requires:
Network Connection
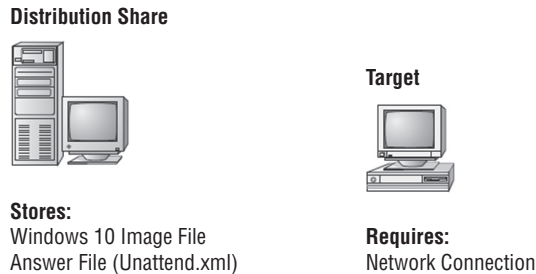
Advantages of Unattended Installation

In a midsize or large organization, it just makes sense to use automated setups. As stated earlier, it is nearly impossible to install Windows 10 one at a time on hundreds of machines. But there are many advantages to using unattended installations as a method for automating Windows 10:

- Unattended installation saves time and money because users do not have to interactively respond to each installation query.

- It can be configured to provide automated query response while still selectively allowing users to provide specified input during installation.

- It can be used to install clean copies of Windows 10 or upgrade an existing operating system (providing it is on the list of permitted operating systems) to Windows 10.

- It can be expanded to include installation instructions for applications, additional language support, service packs, and device drivers.

- The physical media for Windows 10 does not need to be distributed to all computers on which it will be installed.

Disadvantages of Unattended Installation

As stated earlier, a manual installation is not practical for mass installations. But one of the biggest disadvantages to performing an unattended installation is that an administrator does not physically walk through the installation of Windows 10. A client operating system is one of the most important items that you will install onto a machine. As an IT manager and consultant, I have always felt better physically installing a client operating system. This way, if there are any glitches, I can see and deal with them immediately. If something happens during an unattended install, you may never know it, but the end user may experience small issues throughout the lifetime of the machine.

Two other disadvantages of using unattended installations as a method for automating Windows 10 installations are listed here:

- They require more initial setup than a standard installation of Windows 10.

- Someone must have access to each client computer and must initiate the unattended installation process on the client side.

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 10 on client computers.

A WDS server installs Windows 10 on the client computers, as illustrated in Figure 2.8. 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.

FIGURE 2.8 Windows Deployment Services (WDS) uses a WDS server and WDS clients.

WDS Server

Stores:
PXE Boot Files and Boot Images
Windows 10 Boot Images
Answer File(s)

WDS Client

Requires:
PXE-Compatible Boot
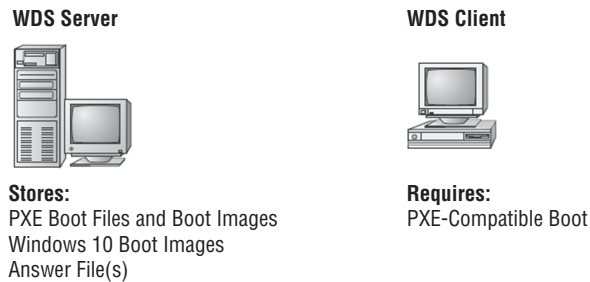
The WDS clients access the network with the help of a Dynamic Host Configuration Protocol (DHCP) server. This allows the WDS client to remotely install the operating system from the WDS server. The network environment must be configured with a DHCP server, a Domain Name System (DNS) server, NTFS Volumes, and Active Directory to connect to the WDS server. No other client operating system 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.

Advantages of WDS

The advantages of using WDS as a method for automating Windows 10 installations are as follows:

- WDS allows an IT department to remotely install Windows operating systems throughout the network. This advantage helps reduce the difficulty and IT manpower cost compared to a manual installation.

- WDS allows an IT department to deploy multiple images for mixed environments including Windows 7, Windows 8, Windows 10, and Windows Server.

- WDS allows IT departments to use Windows setups including Windows Preinstallation Environment (Windows PE), .wim files, and image-based setups.

- WDS uses multicasting to allow for the transmitting data and imaging data to communicate to each other.

- An IT department can create reference images using the Windows Imaging and Configuration Designer (Windows ICD) to customize Windows 10 images.

- WDS allows an IT administrator to install a driver package to the server and configure the drivers to be deployed to client computers at the same time the image is installed.

- WDS allows IT departments to standardize Windows 10 installations throughout a group or organization.

- The physical media for Windows 10 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 10 installations include the following:

- WDS can be used only if your network is running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 with Active Directory installed.

- The clients that use WDS must be PXE compatible or have a discovery image.

You can configure WDS on a Windows Server 2012 or Windows Server 2012 R2 computer by using the Windows Deployment Services Configuration Wizard or by using the WDSUTIL command-line utility. Table 2.1 describes the WDSUTIL command-line options.

TABLE 2.1   WDSUTIL command-line options

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

WDSUTIL Option	Description
/remove	Removes images from the server
/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-image	Copies images from the image store
/export-image	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-autoadddevices	Approves Auto-Add devices
/reject-autoadddevices	Rejects Auto-Add devices
/delete-autoadddevices	Deletes records from the Auto-Add database
/update	Uses a known-good resource to update a server resource

An Overview of the System Preparation Tool and Disk Imaging

The *System Preparation Tool,* or *Sysprep* (Sysprep.exe), is used to prepare a computer for disk imaging, and the disk image can then be captured using Image Capture Wizard (an imaging-management tool included with Windows 10) or third-party imaging software. Sysprep is a free utility that comes on all Windows operating systems. By default, the Sysprep utility can be found on Windows Server 2012 R2 and Windows 10 operating systems in the \Windows\system32\sysprep directory.

   Disk imaging is the process of taking a checkpoint of a computer and then using that checkpoint to create new computers, thus allowing for automated deployments. The reference, or source, computer has Windows 10 installed and is configured with the settings

and applications that should be installed on the target computers. The image (checkpoint) is then created and can be transferred to other computers, thus installing the operating system, settings, and applications that were defined on the reference computer.

Using Imaging Software

Using the System Preparation Tool and disk imaging is a good choice (and the one most commonly used in the real world) for automatic deployment when you have a large number of computers with similar configuration requirements or machines that need to be rebuilt frequently.

For example, StormWind Studios, an online computer education company, reinstalls the same software every few week for new classes. Imaging is a fast and easy way to simplify the deployment process.

Most organizations use images to create new machines quickly and easily, but they also use them to reimage end users' machines that crash.

In most companies, end users will have space on a server (home folders) to allow them to store data. We give our end users space on the server because this way we need to back up only the servers at night and not the end users' machines. If your end users place all of their important documents on the server, that information gets backed up.

Now, if we are also using images in our company and an end user's machine crashes, we just reload the image and they are backed up and running in minutes. Since their documents are being saved on the server, they do not lose any of their information.

Many organizations use third-party imaging software (such as Ghost) instead of using `Sysprep.exe` and Image Capture Wizard. This is another good way of imaging your Windows 10 machines. Just make sure your third-party software supports the Windows 10 operating system.

To perform an unattended installation, 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 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 (out-of-the-box experience) option with the System Preparation Tool and an answer file named Oobe.xml.

The out-of-the-box experience makes the newly built system work as if you took the new system right out of the manufacturer's box.

Sysprep is a utility that is good only for setting up a new machine. You do not use Sysprep to image a computer for upgrading a current machine. There are a few switches that you can use in conjunction with Sysprep to configure the Sysprep utility for your specific needs. Table 2.2 shows you the important Sysprep switches and what they will do for you when used.

TABLE 2.2 Sysprep switches

Switch	Explanation
/pnp	Forces a mini-setup wizard to start at reboot so that all Plug and Play devices can be recognized.
/generalize	This allows Sysprep to remove all system-specific data from the Sysprep image. If you're running the GUI version of Sysprep, this is a check-box option.
/oobe	Initiates the Windows Welcome screen at the next reboot.
/audit	Initiates Sysprep in audit mode.
/nosidgen	Sysprep does not generate a new SID on the computer restart. Forces a mini-setup on restart.
/reboot	Stops and restarts the computer system.
/quiet	Runs without any confirmation dialog messages being displayed.
/mini	Tells Sysprep to run the mini-setup on the next reboot.

🌐 Real World Scenario

The SID Problem with Deployment Software

For many years, when you had to create many machines that each had a Microsoft operating system on it, you would have to use files to help deploy the multiple systems.

Then, multiple third-party companies came out with software that allowed you to take a picture of the Microsoft operating system, and you could deploy that picture to other machines. One advantage of this is that all the software that is installed on the system

could also be part of that picture. This was a great way to copy all the software on a machine over to another machine.

There was one major problem for years—*security identifier (SID)* numbers. All computers get assigned a unique SID that represents them on a domain network. The problem for a long time was that when you copied a machine to another machine, the SID number was also copied.

Microsoft released Sysprep many years ago, and that helped solve this problem. Sysprep would allow you to remove the SID number so that a third-party software package could image it to another machine. Many third-party image software products now also remove the SID numbers, but Sysprep was one of the first utilities to help solve this problem.

When you decide to use Sysprep to set up your images, there are a few rules that you must follow for Sysprep to work properly:

- You can use images to restart the Windows activation clock. The Windows activation clock starts to decrease as soon as Windows starts for the first time. You can restart the Windows activation clock only three times using Sysprep.

- The computer on which you're running Sysprep has to be a member of a workgroup. The machine can't be part of a domain. If the computer is a member of the domain, when you run Sysprep, the computer will automatically be removed from the domain.

- When installing the image, the system will prompt you for a product key. During the install you can use an answer file, which in turn will have all the information needed for the install, and you will not be prompted for any information.

- A third-party utility or Image Capture Wizard is required to deploy the image that is created from Sysprep.

- If you are using Sysprep to capture an NTFS partition, any files or folders that are encrypted will become corrupt and unreadable.

One advantage to Sysprep and Windows 10 is that you can use Sysprep to prepare a new machine for duplication. You can use Sysprep to image a Windows 10 machine. The following steps are necessary to image a new machine:

1. Install the Windows 10 operating system.

2. Install all components on the OS.

3. Run `Sysprep /generalize` to create the image.

When you image a computer using the Windows Sysprep utility, a Windows image (`.wim`) file is created. Most third-party imaging software products can work with the Windows image file.

Advantages of the System Preparation Tool

The following are advantages of using the System Preparation Tool as a method for auto-mating Windows 10 installations:

- For large numbers of computers with similar hardware, it greatly reduces deploy-ment 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

There are some disadvantages of using the System Preparation Tool as a method for auto-mating Windows 10 installations:

- Image Capture Wizard, third-party imaging software, or hardware disk-duplication devices must be used for an image-based setup.

- The version of the System Preparation Tool that shipped with Windows 10 must be used. An older version of Sysprep cannot be used on a Windows 10 image.

- The System Preparation Tool will not detect any hardware that is not Plug and Play compliant.

Overview of the Windows Assessment and Deployment Kit

Another way to install Windows 10 is to use the *Windows Assessment and Deployment Kit (ADK)*. The Windows ADK is a set of utilities and documentation that allows an administrator to configure and deploy Windows operating systems. An administrator can use the Windows ADK to do the following:

- Windows Imaging and Configuration Designer (ICD)

- Windows Assessment Toolkit

- Windows Performance Toolkit

The Windows ADK can be installed and configured on the following operating systems:

- Windows 10

- Windows 7/8 with SP1

- Windows Server 2012 R2

- Windows Server 2012

- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2003 with SP2

The Windows ADK is a good solution for organizations that need to customize the Windows deployment environments. The Windows ADK allows an administrator to have the flexibility needed for mass deployments of Windows operating systems. Since every organization's needs are different, the Windows ADK allows you to use all or just some of the deployment tools available. It allows you to manage deployments by using some additional tools.

Windows Imaging and Configuration Designer (ICD)   The tools included with this part of the Windows ADK will allow an administrator to easily deploy and configure Windows operating systems and images.

Windows Assessment Toolkit   When new Windows operating systems are installed, applications that ran on the previous version of Windows may not work properly. The Application Compatibility Toolkit allows an administrator to help solve these issues before they occur.

Windows Performance Toolkit   The Windows Performance Toolkit is a utility that will locate computers on a network and then perform a thorough inventory of them. This inventory can then be used to determine which machines can have Windows 10 installed.

Windows Imaging and Configuration Designer

The Windows Imaging and Configuration Designer (ICD) allows an administrator to work with images. The ICD allows an IT department to do the following;

- View and configure all of the settings and policies for a Windows 10 image or provisioning package
- Create Windows provisioning answer files
- Allow an answer file to add third-party drivers, apps, or other assets
- Create variants and specify the settings that apply to each variant
- Build and flash a Windows image
- Build a provisioning package

The Windows ICD gives an IT department many options on how to deploy and set up Windows 10 clients. Here are some of the functions that can be performed with the Windows ICD tools:

- Configure and edit images by using the Deployment Image Servicing and Management (DISM) utility
- Create Windows Preinstallation Environment (Windows PE) images
- Migrate user data and profiles using the User State Migration Tool (USMT)
- Windows Imaging and Configuration Designer (Windows ICD)

Summary of Windows 10 Deployment Options

Table 2.3 summarizes the installation tools and files that are used with unattended, automated installations of Windows 10, the associated installation method, and a description of each tool.

TABLE 2.3 Summary of Windows 10 unattended deployment utilities

Tool or File	Automated Installation Option	Description
Setup.exe	Unattended installation	Program used to initiate the installation process
Autounattend.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
Image Capture Wizard.exe	Sysprep	Command-line utility that works in conjunction with Sysprep to create and manage Windows 10 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 Image Capture Wizard, third-party software, or hardware disk-duplication devices

The Windows 10 installation utilities and resources relating to automated deployment are found in a variety of locations. Table 2.4 provides a quick reference for each utility or resource and its location.

TABLE 2.4 Location of Windows 10 deployment utilities and resources

Utility	Location
Sysprep.exe	Included with Windows 10; installed to %WINDIR%\system32\sysprep
Image Capture Wizard.exe	Installed with the WAIK; installed to C:\ProgramFiles\ Windows AIK\Tools\x86\Image Capture Wizard.exe
Windows System Image Manager	Installed with WAIK; installed to C:\ProgramFiles\Windows AIK\Tools\Image Manager\ ImgMgr.exe

Deploying Unattended Installations

You can deploy Windows 10 installations or upgrades through a Windows 10 distribution DVD or through a distribution server that contains Windows 10 images and associated files, such as `Autounattend.xml` for unattended installations. Using a DVD can be advantageous if the computer on which you want to install Windows 10 is not connected to the network or is connected via a low-bandwidth network. It is also typically faster to install a Windows 10 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 10 image. Answer files are XML files that contain the settings that are typically supplied by the installer during attended installations of Windows 10. Answer files can also contain instructions for how programs and applications should be run.

The Windows Setup program is run to install or upgrade to Windows 10 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 I'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 versions of Windows prior to Windows 7/8. Although it's 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 10:

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

The Windows Setup program has several command-line options that can be applied. Table 2.5 describes the `Setup.exe` command-line options.

TABLE 2.5   `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 troubleshooting 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

Setup.exe Option	Description
/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, Setup will use the default location.
/noreboot	Normally, when the down-level 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 10 and the installation partition for Windows 10.
/unattend:[answerfile]	Specifies that you will be using an unattended installation for Windows 10. The answerfile variable points to the custom answer file you will use for installation.

Next we'll look at the System Preparation Tool (Sysprep); using it is one of many ways to install Windows 10 automatically.

Using the System Preparation Tool to Prepare an Installation for Imaging

You can use disk images to install Windows 10 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 10 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 Image Capture Wizard to create an image of the installation.

The System Preparation Tool (Sysprep.exe) is included with Windows 10, in the %WINDIR%\system32\sysprep directory. When you run this utility on the source computer, it strips out information that is 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 Tool 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
/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 it.

Preparing a Windows 10 Installation

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

1. Install Windows 10 on a source computer. The computer should have a similar hardware configuration to that of the destination computer(s). The source computer should not be a member of a domain. (See Chapter 1 for instructions on installing Windows 10.)

2. Log on to the source computer as 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. Select the appropriate options for your configuration.

6. If configured to do so, Windows 10 will be rebooted into setup mode, and you will be prompted to enter 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.

In Exercise 2.3, you will use the System Preparation Tool to prepare the computer for disk imaging. The Sysprep utility must be run on a machine with a clean version of Windows 10. If you upgraded a Windows 7 or Windows 8 machine to Windows 10, you will not be able to run the Sysprep utility.

EXERCISE 2.3

Preparing a System for Imaging by 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 Enter System Out-Of-Box Experience (OOBE) in the system cleanup action.

4. Under the shutdown options, 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. Choose the Reboot option. Click OK.

5. Configure the Sysprep utility and name the image **`image.wim`**.

After creating the Sysprep image, you need to use some type of third-party software to capture it. Windows includes a utility called Image Capture Wizard for just that purpose.

Using Windows Imaging and Configuration Designer (Windows ICD) 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 Image Capture Wizard, which is a utility that can be used to create and manage Windows image (`.wim`) files.

To run the Image Capture Wizard utility to create a disk image of a Windows 10 installation, follow these steps:

1. From the Windows ICD Start page, select New Windows Image Customization.

2. In the Enter Project Details window, specify a Name and Location for your project. Optionally, you can also enter a brief Description to describe your project.

3. Click Next.

4. If you selected New Windows Image Customization from the Start page, skip this step.

In the Select Project Workflow window, select Imaging from the list of available project workflows and then click Next.

5. In the Select Imaging Source Format window, select "The Windows image is based on a Windows image (WIM) file" and then click Next.

6. In the Select Image window, click Browse to launch File Explorer. Search and locate the path to the `Install.wim` file.

After you've selected the `Install.wim` file, all the Windows images in the `.wim` file are listed in the Available images panel. By default, the first Windows image in the list is selected, and the information about this image is displayed in the Image Information panel.

7. Select the Windows image that you want to use and then click Next.

8. Optional: If you have a provisioning package that contains customizations already configured in a different project and you want to reuse the customizations from this package, click Browse in the Import A Provisioning Package screen to locate the provisioning package that was exported from another project.

9. Click Finish.

There is also a command-line version of the Windows (ICD) tool that you can use. The Microsoft exams have started using a lot of command-line utilities on their tests. So let's take a look at the Windows (ICD) command-line utility. The command that we use for this is `icd.exe`, as follows:

```
icd.exe <command> <parameters>
```

Table 2.7 describes some of the `icd.exe` command switches that you can use to configure the images.

TABLE 2.7 icd.exe switches

Switch	Description
/CustomizationXML	Identifies the location of the Windows provisioning XML file. This file holds the information for customization assets and settings.
/PackagePath	Identifies the location and the built provisioning package name where the package will be saved.
/StoreFile	Allows IT administrators to use their own settings store instead of the default store used by Windows ICD. If an IT administrator does not determine his or her own store, a default store that's common to all Windows editions will be loaded by Windows ICD.

Switch	Description
`/MSPackageRoot`	Identifies the location of the root directory that holds the Microsoft packages that you downloaded from the Windows portal.
`/OEMInputXML`	Identifies the location to the `OEMInput.xml` file. This file defines a subset of settings that can be designed based on the image type.
`/Variables`	Identifies a macro pair that is separated by a semicolon, *<name>* and *<value>*.
`Encrypted`	Indicates whether or not the provisioning package should be created with encryption. Windows ICD will then automatically generate a decryption password that is included with the output.
`Overwrite`	Indicates whether or not to overwrite the existing provisioning package.
`/?`	Used to access the ICD help, which lists the switches and their descriptions for the ICD command-line tool.

After you create the disk image, the next step is to install it. In the next section, you'll learn how to install the disk image on a new machine.

Installing from a Disk Image

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

Once 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 Image Capture Wizard 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, the computer name, and the password to the new computer after the destination computer is rebooted.

In Exercise 2.4, you will use the stripped image that was created in Exercise 2.3 to simulate the process of continuing an installation from a disk image.

Installing Windows 10 from a Disk Image

1. Boot the target computer into Windows PE.

2. Copy the image created in Exercise 2.3 to the local computer by using the following commands:

   ```
   net use z: \\Server\Images
   copy  Z:\Images\image.wim E:
   ```

3. Apply the image to the target computer using the following Image Capture Wizard command:

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

When you install Windows 10, the installation wizard asks you questions such as your username and computer name. There is a way to answer these questions without actually being in front of the computer.

Using the Deployment Image Servicing and Management Tool

Deployment Image Servicing and Management (DISM.exe) is a command-line utility that allows you to manipulate a Windows image. DISM also allows you to prepare a Windows PE image. DISM replaces multiple programs that were included with Windows 7/8. These programs include Package Manager (Pkgmgr.exe), PEimg, and Intlcfg. These tools have been consolidated into one tool (DISM.exe), and new functionality has been added to improve the experience for offline servicing.

DISM provides additional functionality when used with Windows 10 and Windows Server 2012 R2. You can use DISM to do the following:

- Add, remove, and enumerate packages
- Add, remove, and enumerate drivers
- Enable or disable Windows features
- Apply changes to an Unattend.xml answer file
- Configure international settings
- Upgrade a Windows image to a different edition
- Prepare a Windows PE 3.0 image

DISM works with all platforms (32-bit, 64-bit, and Itanium) and allows for the use of Package Manager scripts.

Table 2.8 describes the commands that can be used with DISM.exe.

TABLE 2.8   `DISM.exe` command-line commands

Command	Description
`/Add-Driver`	Adds third-party driver packages to an offline Windows image.
`/Get-CurrentEdition`	Displays the edition of the specified image.
`/Get-Drivers`	Displays basic information about driver packages in the online or offline image. By default, only third-party drivers will be listed.
`/Get-DriverInfo`	Displays detailed information about a specific driver package.
`/Get-Help /?`	Displays information about the option and the arguments.
`/Get-TargetEditions`	Displays a list of Windows editions that an image can be changed to.
`/Remove-Driver`	Removes third-party drivers from an offline image.
`/Set-ProductKey:<productKey>`	Can only be used to enter the product key for the current edition in an offline Windows image.

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 10 installation. You can use answer files with Windows 10 unattended installations, disk image installations, or WDS installations. Setting up answer files allows you to easily deploy Windows 10 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 (Windows 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 drivers in 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 an 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 which 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 be applied only 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 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.

Understanding Hyper-V

In the following sections, I'll introduce you to Hyper-V. To begin, we'll take a look at virtualization and what types of virtualization exist. We will then discuss Hyper-V features and the Hyper-V architecture before finishing up with the Hyper-V requirements for software and hardware.

Hyper-V is very important to understand when working with Windows 10 because you can load a Windows 10 guest virtual machine onto a Hyper-V host system and you also have the ability to use Windows 10 as a Windows Hyper-V host.

Let's first make sure you understand what host and guest systems do. The Hyper-V machine that has another operating system running on top of it is a host. If you are running an operating system on top of another operating system, you are the guest system. So Windows 10 can be set up as a Hyper-V host or a Hyper-V guest.

So if you are running Windows Server 2012 R2 Hyper-V and the computer has issues, you can load the Server 2012 R2 Hyper-V virtual machines onto a Windows 10 Hyper-V host system. This gives you a temporary solution while the Windows Server 2012 R2 Hyper-V server gets repaired.

So why are we talking about Hyper-V in a Windows 10 deployment chapter? Because you can build a Windows 10 virtual machine and use that virtual machine to deploy Windows 10 operating systems throughout an organization.

What Is Virtualization?

Virtualization is a method for abstracting physical resources from the way they interact with other resources. For example, if you abstract the physical hardware from the operating system, you get the benefit of being able to move the operating system between different physical systems.

This is called *server virtualization*. But there are also other forms of virtualization available, such as presentation virtualization, desktop virtualization, and application virtualization. I will now briefly explain the differences between these forms of virtualization:

Server Virtualization   This basically enables multiple operating systems to run on the same physical server. Hyper-V is a server virtualization tool that allows you to move physical machines to virtual machines and manage them on a few physical servers. Thus, you will be able to consolidate physical servers.

Presentation Virtualization   When you use *presentation virtualization*, your applications run on a different computer and only the screen information is transferred to your computer. An example of presentation virtualization is Microsoft Remote Desktop Services in Windows Server 2012 R2.

Desktop Virtualization   *Desktop virtualization* provides you with a virtual machine on your desktop, comparable to server virtualization. You run your complete operating system and applications in a virtual machine so that your local physical machine just needs to run a very basic operating system. An example of this form of virtualization is Microsoft Windows 10 Hyper-V.

Application Virtualization   *Application virtualization* helps prevent conflicts between applications on the same PC. Thus, it helps you to isolate the application running environment from the operating system installation requirements by creating application-specific copies of all shared resources, and it helps reduce application-to-application incompatibility and testing needs. An example of an application virtualization tool is Microsoft Application Virtualization (App-V).

Installing the Hyper-V Role

Now it's time to see how to install the Hyper-V server role on both a Windows Server machine and a Windows 10 client. I'll show you how to install Hyper-V onto a Windows Server 2012 R2 system as well as how to load Hyper-V onto a Windows 10 Enterprise System.

So why am I showing both installations? Because you can load Windows 10 onto a Windows Server 2012 R2 Hyper-V server and you can use Windows 10 as a Hyper-V server.

Installing Hyper-V in Windows Server 2012 R2

You can install the Hyper-V server role on any Windows Server 2012 R2 installation. The server must meet both the hardware and software requirements. The installation process is simple, as Exercise 2.5 demonstrates.

EXERCISE 2.5

Installing Hyper-V in Windows Server 2012 R2

1. Open Server Manager.

2. In Server Manager, choose number 2, Add Roles And Features.

3. At the Select Installation Type page, choose the role-based or feature-based installation. Click Next.

4. On the Select Destination Server screen, choose Select A Server From The Server Pool and choose the server to which you want to add this role. Click Next.

5. On the Select Server Roles screen, click the check box next to Hyper-V. When the Add Features dialog box appears, click the Add Features button. Then click Next.

6. At the Select Features screen, just click Next.

7. At the Hyper-V introduction screen, just click Next.

8. At the Create Virtual Switches screen, choose your adapter and click Next.

9. At the Virtual Machine Migration screen, just click Next. You want to use migration only if you have multiple Hyper-V servers. Since we will have only one for this exercise, just skip this screen.

10. At the Default Stores screen, accept the defaults and click Next.

11. At the Confirmation screen, click the Install button.

12. After the installation is complete, click the Close button.

13. Restart your server.


Installing Hyper-V in Windows 10

You can install the Hyper-V server role on any Windows 10 Professional or Enterprise installation. The Windows 10 system must meet both the hardware and software requirements. The installation process is shown in Exercise 2.6.

EXERCISE 2.6

Installing Hyper-V on Windows 10

1. Right-click the Windows button and select Programs And Features.

2. Select the Turn Windows Features On Or Off option.

3. Select Hyper-V and click OK (as shown in Figure 2.9).

FIGURE 2.9   Installing Hyper-V
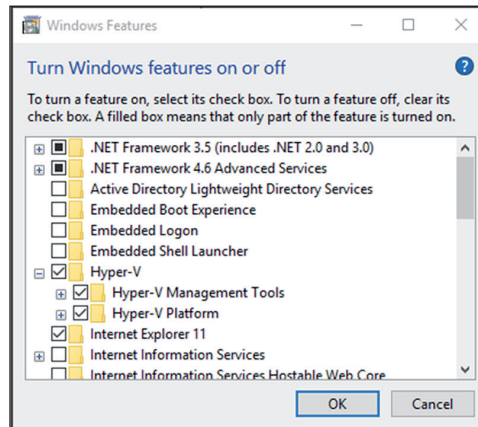
4. After the installation is complete, click the Close button.

5. Restart your system.

Now that you know how to install the Hyper-V roles onto a Windows 10 system using Programs And Features, let's install Hyper-V onto Windows 10 by using PowerShell. The following command is run in Windows PowerShell:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V –All
```

The following PowerShell command is used to install Hyper-V into a Windows 10 image while it's an actual image:

```
DISM /Online /Enable-Feature /All /FeatureName:Microsoft-Hyper-V
```

Using Hyper-V Manager

Hyper-V Manager is the central management console to configure your server and create and manage your virtual machines, virtual networks, and virtual hard disks. Unlike Virtual Server 2005, where you managed all virtual machines through a web interface, Hyper-V Manager is managed through a Microsoft Management Console (MMC) snap-in.

You can access it by right-clicking the Start button ➤ Control Panel ➤ Administrative Tools ➤ Hyper-V Manager. Figure 2.10 shows how Hyper-V Manager looks once you start it.

FIGURE 2.10   Hyper-V Manager
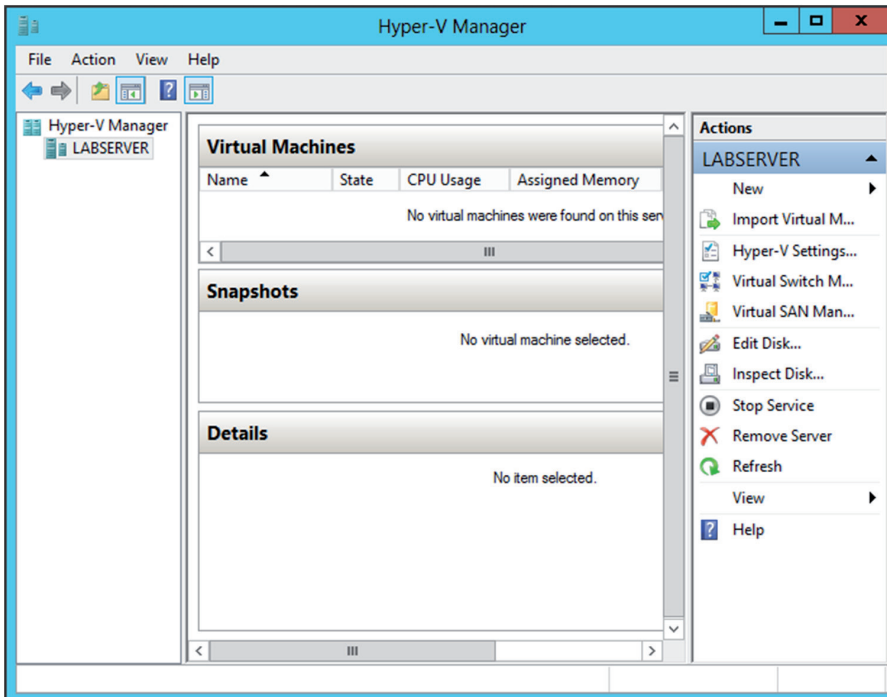
Manage Virtual Switches

A virtual network provides the virtual links between nodes in either a virtual or physical network. Virtual networking in Hyper-V is provided in a secure and dynamic way because you can granularly define virtual network switches for their required usage. For example, you can define a private or internal virtual network if you don't want to allow your virtual machines to send packets to the physical network.

To allow your virtual machines to communicate with each other, you need virtual networks. Just like normal networks, virtual networks exist only on the host computer and allow you to configure how virtual machines communicate with each other, with the host, and with the network or the Internet. You manage virtual networks in Hyper-V using Virtual Switch Manager.

Using Virtual Switch Manager, you can create, manage, and delete virtual switches. You can define the network type as external, internal only, or private.

External   Any virtual machine connected to this virtual switch can access the physical network. You would use this option if you want to allow your virtual machines to access, for example, other servers on the network or the Internet. This option is used in production environments where your clients connect directly to the virtual machines.

Internal   This option allows virtual machines to communicate with each other as well as the host system but not with the physical network. When you create an internal network, it also creates a local area connection in Network Connections that allows the host machine to communicate with the virtual machines. You can use this if you want to separate your host's network from your virtual networks.

Private   When you use this option, virtual machines can communicate with each other but not with the host system or the physical network; thus, no network packets are hitting the wire. This option allows virtual machines on the same Hyper-V host to communicate without using any network traffic.

On the external and internal-only virtual networks, you also can enable virtual LAN (VLAN) identification. You can use VLANs to partition your network into multiple subnets using a VLAN ID. When you enable virtual LAN identification, the NIC that is connected to the switch will never see packets tagged with VLAN IDs. Instead, all packets traveling from the NIC to the switch will be tagged with the access mode VLAN ID as they leave the switch port. All packets traveling from the switch port to the NIC will have their VLAN tags removed. You can use this if you are already logically segmenting your physical machines and also use it for your virtual ones.

Managing Virtual Hard Disks

In addition to virtual networks, you need to manage virtual hard disks that you attach to your virtual machines. A virtual hard disk in Hyper-V, apart from a pass-through disk, is a VHD or VHDX file that basically simulates a hard drive on your virtual machine.

The following sections will first show you what types of virtual hard disks are available and then show you how to create them. You will also learn about what options are available to manage virtual hard disks.

Types of Hard Disks

Depending on how you want to use the disk, Hyper-V offers various types, as described in Table 2.9.

TABLE 2.9   Types of virtual hard disks

Type of Disk	Description	When to Use It
Dynamically expanding	This disk starts with a small VHD file and expands it on demand once an installation takes place. It can grow to the maximum size you defined during creation. You can use this type of disk to clone a local hard drive during creation.	This option is effective when you don't know the exact space needed on the disk and when you want to pre-serve hard disk space on the host machine. Unfortunately, it is the slowest disk type.
Fixed size	The size of the VHD file is fixed to the size specified when the disk is created. This option is faster than a dynamically expanding disk. However, a fixed-size disk uses up the maximum defined space immediately. This type is ideal for cloning a local hard drive.	A fixed-size disk provides faster access than dynami-cally expanding or differenc-ing disks, but it is slower than a physical disk.
Differencing	This type of disk is associated in a parent-child relationship with another disk. The differencing disk is the child, and the associated vir-tual disk is the parent. Differencing disks include only the differences to the parent disk. By using this type, you can save a lot of disk space in similar virtual machines. This option is suitable if you have multiple virtual machines with the same operating systems.	Differencing disks are most commonly found in test environments and should not be used in production environments.
Physical (or pass-through disk)	The virtual machine receives direct pass-through access to the physical disk for exclusive use. This type provides the highest per-formance of all disk types and thus should be used for production servers where performance is the top priority. The drive is not avail-able for other guest systems.	This type is used in high-end data centers to provide opti-mum performance for VMs. It's also used in failover cluster environments.

Creating Virtual Hard Disks

To help you gain practice in creating virtual hard disks, the following three exercises will teach you how to create a differencing hard disk, how to clone an existing disk by creating a new disk, and how to configure a physical or pass-through disk to your virtual machine. First, in Exercise 2.7, you will learn how to create a differencing virtual hard disk.

EXERCISE 2.7

Creating a Differencing Hard Disk

1.   Open Hyper-V Manager.

2.   In Hyper-V Manager, on the Actions pane, choose New ➢ Hard Disk.

3.   In the New Virtual Hard Disk Wizard, click Next on the Before You Begin page.

4.   On the Choose Disk Format screen, choose VHDX and click Next. The size of your VHDs determines which format you should choose. If you're going to have a VHD larger than 2 TB, use VHDX. If your VHD is less than 2 TB, then you should use VHD.

5.   On the Choose Disk Type page, select Fixed Size and click Next.

6.   On the Specify Name And Location page, enter the new name of the child disk (for example, `newvirtualharddisk.vhd`). You can also modify the default location of the new VHD file if you want. Click Next to continue.

7.   Next, on the Configure Disk page, you need to specify the size of the VHD file. Choose a size based on your hard disk and then click Next to continue. I used 60 GB as the test size.

8.   On the Completing The New Virtual Hard Disk Wizard page, verify that all settings are correct, and click Finish to create the hard disk.

Changing Virtual Hard Disks

Hyper-V also provides two tools to manage virtual hard disks: Inspect Disk and Edit Disk. These tools are available on the Actions pane in Hyper-V Manager:

Inspect Disk   This provides you with information about the virtual hard disk. It shows you not only the type of the disk but also information like the maximum size for dynamically expanding disks and the parent VHD for differencing disks.

Edit Disk   This provides you with the Edit Virtual Hard Disk Wizard, which you can use to compact, convert, expand, merge, or reconnect hard disks.

Table 2.10 provides an overview of what you can do with the wizard.

TABLE 2.10   Edit Disk overview

Action	Description
Compact	Reduces the size of a dynamically expanding or differencing disk by removing blank space from deleted files.
Convert	Converts a dynamically expanding disk to a fixed disk or vice versa.

TABLE 2.10   Edit Disk overview *(continued)*

Action	Description
Expand	Increases the storage capacity of a dynamically expanding disk or a fixed virtual hard disk.
Merge	Merges the changes from a differencing disk into either the parent disk or another disk (applies to differencing disks only!).
Reconnect	If a differencing disk does not find its referring parent disk anymore, this option can reconnect the parent to the disk.

Configuring Virtual Machines

The following sections cover the topics of creating and managing virtual machines as well as how to back up and restore virtual machines using features like Import and Export and Checkpoints.

Creating and Managing Virtual Machines

It is important to learn how to create a virtual machine, how to change its configuration, and how to delete it. We will take a look at the Virtual Machine Connection tool and install the Hyper-V Integration Components onto a virtual machine.

Virtual machines define the child partitions in which you run operating system instances. Each virtual machine is separate and can communicate with the others only by using a virtual network. You can assign hard drive(s), virtual network(s), DVD drives, and other system components to it. A virtual machine is similar to an existing physical server, but it doesn't run on dedicated hardware anymore—it shares the hardware of the host system with the other virtual machines that run on the host.

Exercise 2.8 shows you how to create a new virtual machine.

EXERCISE 2.8

Creating a New Virtual Machine

1. Open Hyper-V Manager.

2. In Hyper-V Manager, on the Actions pane, choose New ➢ Virtual Machine.

3. In the New Virtual Machine Wizard, click Next on the Before You Begin page.

4. On the Specify Name And Location page, give your virtual machine a name and change the default location of the virtual machine configuration files. Click Next to continue.

5. On the Assign Memory page, define how much of your host computer's memory you want to assign to this virtual machine. Remember that once your virtual machine uses up all your physical memory, it will start swapping to disk, thus reducing the performance of all virtual machines. Click Next to continue.

6. On the Configure Networking page, select the virtual network that you previously configured using Virtual Network Manager. Click Next to continue.

7. On the next page, you configure your virtual hard disk. You can create a new virtual hard disk, select an existing disk, or choose to attach the hard disk later. Be aware that you can create only a dynamically expanding virtual disk on this page; you cannot create a differencing, physical, or fixed virtual hard disk here. However, if you created the virtual hard disk already, you can, of course, select it. Click Next to continue.

8. On the Installation Options page, you can select how you want to install your operating system. You have the option to install an operating system later, install the operating system from a boot CD/DVD-ROM where you can select a physical device or an image file (ISO file), install an operating system from a floppy disk image (VFD file, or a virtual boot floppy disk), or install an operating system from a network-based installation server. The last option will install a legacy network adapter to your virtual machine so you can boot from the network adapter. Select Install An Operating System Later and then click Next.

9. On the Completing The New Virtual Machine Wizard summary page, verify that all settings are correct. You also have the option to immediately start the virtual machine after creation. Click Next to create the virtual machine.

10. Repeat this process and create a few more virtual machines.

11. If you want to install an operating system on one of the VMs, start the VM, load a Windows 10 installation disk into the DVD, and then under the Media menu, choose DVD and Capture. Then just do a normal install.

After completing Exercise 2.8, you will have a virtual machine available in Hyper-V Manager. Initially, the state of the virtual machine will be Off. Virtual machines can have the following states: Off, Starting, Running, Paused, and Saved. You can change the state of a virtual machine in the Virtual Machines pane by right-clicking the virtual machine's name or by using the Virtual Machine Connection window.

Here is a list of some of the state options (when the VM is running) available for a virtual machine:

Start   Turn on the virtual machine. This is similar to pressing the power button when the machine is turned off. This option is available when your virtual machine is off or in saved state.

Turn Off   Turn off the virtual machine. This is similar to pressing the power off button on the computer. This option is available when your virtual machine is in running, saved, or paused state.

Shut Down   This option shuts down your operating system. You need to have the Hyper-V Integration Components installed on the operating system; otherwise, Hyper-V will not be able to shut down the system.

Save   The virtual machine is saved to disk in its current state. This option is available when your virtual machine is running or in paused state.

Pause   Pause the current virtual machine, but do not save the state to disk. You can use this option to quickly release processor utilization from this virtual machine to the host system.

Reset   Reset the virtual machine. This is like pressing the reset button on your computer. You will lose the current state and any unsaved data in the virtual machine. This option is available when your virtual machine is running or in paused state.

Resume   When your virtual machine is paused, you can resume it and bring it online again.

Installing Hyper-V Integration Components

Hyper-V Integration Components, also called Integration Services, are required to make your guest operating system "hypervisor aware." These components improve the performance of the guest operating system once the components are installed. On the architectural perspective, virtual devices are redirected directly via the VMBus; thus quicker access to resources and devices is provided.

If you do not install the Hyper-V Integration Components, the guest operating system uses emulation to communicate with the host's devices, which of course makes the guest operating system slower.

Exercise 2.9 shows you how to install Hyper-V Integration Components on one of your virtual machines running Windows 10.

EXERCISE 2.9

Installing Hyper-V Integration Components

1.   Open Hyper-V Manager.

2.   In Hyper-V Manager, in the Virtual Machines pane, right-click the virtual machine on which you want to install Hyper-V Integration Components and select Start.

3.   Right-click the virtual machine again and select Connect. Meanwhile, your virtual machine should be already booting.

4.   If you need to log in to the operating system of your virtual machine, you should do so.

5.   Once the Windows desktop appears, you need to select Insert Integration Services Setup Disk from the Actions menu of your Virtual Machine Connection window.

6.   Once the Hyper-V Integration Components are installed, you are asked to perform a reboot.

After the reboot, Hyper-V Integration Components are installed on your operating system, and you will be able to use them.

Managing Checkpoints

With virtual machine checkpoints (formerly known as virtual machine snapshots), you can save a copy of the virtual machine at any point in time, including while the virtual machine is running. You can take multiple checkpoints of a virtual machine and then revert it to any previous state by applying a checkpoint.

Using checkpoints makes it easier to diagnose the cause of errors by reducing the number of times you need to repeat a task or sequence within a virtual machine. The benefit is obvious; if you use checkpoints to revert to a previous virtual machine configuration, you do not need to copy virtual machines to keep a state. Thus, it is a quick and easy way to back up a certain state of your virtual machine.

You can create a checkpoint when a virtual machine is in a running, saved, or turned-off state. It's only from a paused state that you cannot perform a checkpoint.

In Exercise 2.10, you'll create and rename a checkpoint.

EXERCISE 2.10

Creating a Checkpoint of a Virtual Machine

1. Open Hyper-V Manager.

2. In Hyper-V Manager, in the Virtual Machines pane, right-click the virtual machine.

3. Select Checkpoints.

4. Once the checkpoint is taken, it should appear in the Checkpoints pane in Hyper-V Manager. Right-click the checkpoint and select Settings.

5. In the Settings window, on the Management pane, click Name and type in **First CheckPoint** as the name. You can also add some notes to make it easy to identify.

6. Click OK to apply the changes. You will now see that the checkpoint has a new name.

Technically speaking, when you make a checkpoint, the following files will be created in the virtual machine's checkpoints folder:

- A virtual machine configuration file
- Virtual machine saved state files
- Checkpoints differencing disks (AVHDs)

Once you create a checkpoint for a virtual machine, you will also have the Revert option available in the virtual machine name's pane in Hyper-V Manager. Reverting basically means that you restore the last checkpoint made. You'll also see the last checkpoint taken marked with a green arrow in the Checkpoints pane.

Settings　This opens the Settings window of the virtual machine. The only settings you can change are the Name and Notes fields. All others are read-only.

Apply　Applying a checkpoint to a virtual machine technically means that you copy the virtual machine state from the checkpoints to the active virtual machine. You can look at

this as a "restore this checkpoint" option. Because you would lose all unsaved data and settings from the active virtual machine, you will be asked if you want to create another checkpoint before you apply this checkpoint. If you just click Apply, the active machine will be overwritten and reverted to the state it was in when the checkpoints was made. This checkpoint will not be removed.

Export This allows you to export the checkpoint to another location.

Rename You can change the name of the checkpoint without the need to open the settings.

Delete Checkpoints Deleting a checkpoint is like deleting a backup file. You will no longer be able to restore to that point in time. Deleting a single checkpoint does not affect any other checkpoints that you made for this virtual machine. You will delete only the selected checkpoints. However, sometimes when you do delete a checkpoint, the system needs to merge the differencing disks. This occurs in the background when the virtual machine is not running. The user does not see when it happens.

Delete Checkpoints Subtree This will delete the selected checkpoints and all checkpoints that are hierarchically underneath it. If you delete a checkpoint with only one sub-checkpoint, the configuration and saved state files for the checkpoints will be deleted and the checkpoint's differencing disks will be merged. If you have more sub-checkpoints, merging will not take place.

In Exercise 2.11, you will apply a checkpoint and thus revert to a previous virtual machine state.

EXERCISE 2.11

Applying a Checkpoint

1. Open Hyper-V Manager.

2. In Hyper-V Manager, in the Virtual Machines pane, click the virtual machine for which you created a checkpoint.

3. In the Checkpoints pane, select First Checkpoints.

4. In the First Checkpoints pane, under Actions, click Apply.

5. In the Apply Checkpoints window, click Apply.

Moving Virtual Machines

There may be time when you need to move a virtual machine or its storage to another server or location. In this section, we will look at how move virtual machines and storage.

Using Hyper-V, you cannot move the configuration files anymore. You need to use the Export feature to export the virtual machine and then use Import on the target machine to import the virtual machine to Hyper-V.

To export a virtual machine, it must be in either Off or Saved state. Open Hyper-V Manager, select the virtual machine you want to export, and either right-click the virtual machine and select Export or click Export on the virtual machine name's pane.

In this window, you can set the export path for the virtual machine and choose whether to export your virtual machine state data or not.

Once you check Don't Export Virtual Machine State Data, only the virtual machine's configuration files will be exported. The virtual hard disk and snapshots will not be exported.

In the export path, a folder with the name of the virtual machine is created along with the following subfolders:

Virtual Machines   This includes the virtual machine configuration files as well as the virtual machine state if the machine is saved.

Virtual Hard Disks   If you exported the state data, this folder will include your virtual hard disks VHD file(s).

Snapshots   If you exported the state data, this folder will include all snapshot files.

Once the virtual machine finishes exporting, you can move the export folder to the target machine if you did not store it directly on the server's disks. Open Hyper-V Manager and click Import Virtual Machine, which is located in the Actions pane.

The Import Virtual Machine dialog box asks you for the path to the exported virtual machine and allows you to decide if you want to reuse the old virtual machine ID.

You want to reuse old virtual machine IDs if you're moving all virtual machines from a host to a new target machine. The virtual machines are practically the same as on the source system. However, you do not want to reuse old virtual machine IDs if you used Export to clone a virtual machine.

When you import a virtual machine with state data, Hyper-V will use the import path for the virtual hard disks as well as snapshots in its virtual machine configuration XML. Thus, you're able to import an exported machine only once. For that reason, the import folder should already be on the host's target disk.

Summary

In this chapter, we discussed automated installation of Windows 10. Installing Windows 10 through an automated process is an effective way to install the Windows 10 operating system on multiple computers.

There are several methods for automated installation: unattended installations, Windows Deployment Services (WDS), Windows Assessment and Deployment Kit (ADK), third-party applications, unattended installations, and using the System Preparation Tool along with Image Capture Wizard.

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 10 on client computers.

The Windows 10 Assessment and Deployment Kit (ADK) is a set of utilities and documentation that allows an administrator to configure and deploy Windows operating systems.

You can use unattended answer files to automatically respond to the queries that are generated during the normal installation process.

You can also prepare an installation for imaging by using the System Preparation Tool (Sysprep.exe) and creating a disk image by using the Image Capture Wizard utility or a third-party utility.

Microsoft Deployment Toolkit (MDT) 2013 Update 1 is a way of automating desktop and server deployment. With the MDT, an administrator can deploy desktops and servers through the use of a common console, which allows for quicker deployments, having standardized desktop and server images and security and zero-touch deployments of Windows 10, Windows 8, Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

Video Resources

There are videos available for the following exercises:

> 2.1
>
> 2.3

You can access the videos at www.wiley.com/go/sybextestprep on the Other Study Tools tab.

Exam Essentials

Know the difference between the various unattended installation methods.   Understand the various options available for unattended installations of Windows 10 and when it is appropriate to use each installation method.

Understand the uses for Hyper-V.   Hyper-V is one way that Windows 10 can be deployed and tested as a guest on a Hyper-V server. You can also run Windows 10 as a host system and run other virtual machines from Windows 10.

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 10 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 them.

Understand the Microsoft Deployment Toolkit (MDT) 2013 Update 1.   Know that the MDT is a way of automating desktop and server deployment. Understand that the MDT allows an administrator to deploy desktops and servers through the use of a common console.

Review Questions

1. You are the network administrator for your organization. You have a reference computer that runs Windows 10. You need to create and deploy an image of the Windows 10 computer. You create an answer file named `answer.xml`. You have to make sure the installation applies the answer file after you deploy the image. Which command should you run before you capture the image?

    A. `ICD.exe /append answer.xml/check`

    B. `ICD.exe /mount answer.xml/verify`

    C. `Sysprep.exe/reboot/audit/unattend:answer.xml`

    D. `Sysprep.exe/generalize/oobe/unattend:answer.xml`

2. You have a Windows 10 Windows Image (WIM) that is mounted. You need to view the list of third-party drivers installed on the WIM. What should you do?

    A. Run DISM and specify the `/get-drivers` parameter.

    B. Run `Driverquery.exe` and use the `/si` parameter.

    C. From Device Manager, view all hidden drivers.

    D. From Windows Explorer, open the `mount` folder.

3. You are the network administrator for a large organization. You are in charge of developing a plan to install 200 Windows 10 computers in your company's data center. You decide to use WDS. You are using a Windows Server 2012 R2 domain and have verified that your network meets the requirements for using WDS. What command-line utility should you use to configure the WDS server?

    A. Image Capture Wizard

    B. WDSUTIL

    C. `Setup.exe`

    D. The WDS icon in Control Panel

4. Will 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 10 installed. Will wants to use WDS for the installations. To fully automate the installations, he needs to create an answer file. Will 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. Image Capture Wizard

    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, the

machines all receive a 169.254.x.x number along with an error. 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 Image Capture Wizard to deploy disk images. Which Windows 10 utility can you use in conjunction with Image Capture Wizard 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 10 within your company. Which of the following options is *not* an advantage to using a WDS automated installation?

A. The Windows 10 security is retained when you restart the computer.

B. Windows 10 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 XYZ Corporation. You are in charge of developing an automated deployment strategy for rolling out new Windows 10 computers. You want to install a WDS server and are evaluating whether an existing server can be used as a WDS server for Windows 10 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 10 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 an 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`

Chapter

3

Configuring Storage and Security

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Support data storage.**

- This objective may include but is not limited to the following subobjectives: identifying and resolving issues related to the following: DFS client including caching settings, storage spaces including capacity and fault tolerance, OneDrive.

✓ **Configure file and folder access.**

- This objective may include but is not limited to the following subobjectives: encrypt files and folders by using EFS, configure NTFS permissions, configure disk quotas, configure file access auditing, configure authentication and authorization.

✓ **Support data security.**

- This objective may include but is not limited to the following subobjectives: encrypting File System (EFS) including Data Recovery Agent.

As you've probably noticed, there are a few different Microsoft objectives covered for the Microsoft Windows 10 (70-697) exam in this chapter. Not only are these topics important for the exam, but properly configuring your storage is a task that every IT professional should know how to accomplish because an improperly configured storage device can cause many issues for an IT team.

When you install Windows 10, you designate the initial configuration for your disks. Through Windows 10'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 as FAT32. You can also convert a FAT32 partition to NTFS. This chapter covers the features of each file system and how to use the Convert utility to convert to NTFS.

Another factor in disk management is choosing the configuration for your physical drives. Windows 10 supports basic, dynamic, and GUID Partition Table (GPT) disks. Dynamic disks are supported by Windows 10, Windows 8, Windows 7, Windows XP Professional, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. Dynamic disks allow you to create simple volumes, spanned volumes, and striped volumes. If your system is configured as a Basic Disk, in order to utilize volumes, you must first convert the machine's basic disks to dynamic disks.

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 multiple types of storage and how to convert from basic storage to dynamic storage.

The other disk-management features covered in this chapter are data compression, data encryption (EFS), disk defragmentation, disk cleanup, and disk error checking.

Understanding File Systems

A partition is a logical division of hard-drive space. Each partition you create under Windows 10 must have a file system associated with it. Partitions allow a single physical hard drive to be represented in the operating system as multiple drive letters and to be used as if there were multiple hard drives installed in the machine.

When selecting a file system, you can select FAT32 or NTFS. You typically select a file system 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 track the storage of files on your hard drive in a way that is easily understood by end users while still allowing the operating system the ability to retrieve the files as requested. One of the fundamental choices associated with file management is the choice of your file system's configuration. It is recommended that you use the NTFS file system with Windows 10 because doing so will allow you to take advantage of features such as local security, file compression, and file encryption. You should choose the FAT32 file system only if you want to dual-boot your computer with a version of Windows that does not support NTFS because FAT32 is backward compatible with other operating systems.

Table 3.1 summarizes the capabilities of each file system, and they are described in more detail in the following sections. These volume size numbers are the current values at the time this book was written. Make sure you continue to check with Microsoft to see if the volume sizes have increased since this book's publication.

TABLE 3.1   File-system capabilities

Feature	FAT32	NTFS
Supporting operating systems	All Windows operating systems above Windows 95	Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2
Long filename support	Yes	Yes
Efficient use of disk space	Yes	Yes
Compression support	No	Yes
Encryption support	No	Yes
Support for local security	No	Yes
Support for network security	Yes	Yes
Maximum volume size	32 GB	16 TB with 4 KB clusters or 256 TB with 64 KB clusters

Windows 10 also supports Compact Disk File System (CDFS). However, CDFS cannot be managed. It is used only to mount and read CDs. Let's start looking at the supported disk file systems.

FAT32

FAT32 is an updated version of File Allocation Table (FAT). The FAT32 version was first shipped with Windows 95 OSR2 (Operating System Release 2) and can be used by every Windows operating system since.

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 512 MB up to 2 TB, although if you create and format a FAT32 partition through Windows 10, the FAT32 partition can only be up to 32 GB. Because of the smaller cluster sizes, FAT32 can also load programs up to 50 percent faster than FAT16 partitions can.

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 doesn't offer native support for disk compression. Now that you understand FAT32, let's take a look at NTFS.

NTFS

NTFS, which was first used with the NT operating system, offers the highest level of service and features for Windows 10 computers. NTFS partitions can be up to 16 TB with 4 KB clusters or 256 TB with 64 KB clusters.

NTFS offers comprehensive folder-level 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 10 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. This is not possible on a FAT32 file system.

NTFS also offers disk-management features—such as compression and encryption capabilities—and data-recovery features. The disk-management features are covered later in this chapter. The data-recovery features are covered in Chapter 10, "Configuring Recovery."

You should also be aware that there are several different versions of NTFS. Every version of Windows 2000 uses NTFS 3.0. Windows 7/8/10, Windows Vista, Windows XP, Windows Server 2003, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2 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 10 computers can access NTFS 3.0 volumes. NTFS 3.1 includes the following features:

- 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 are 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.

- It gives you the ability to resize volumes and partitions.

- You can use recovery logging on NTFS metadata, which is used for data recovery when a power failure or system problem occurs.

Now that you have seen the differences between FAT32 and NTFS, let's discuss how to convert a FAT32 drive to an NTFS drive.

File System Conversion

In Windows 10, 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 opposed to converting it, 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 it contains the Windows 10 operating system files or the system's page file—the conversion will not take place until the computer is restarted.

In Exercise 3.1, you will convert your D: drive from FAT32 to NTFS. For this exercise, it is assumed that you have a D: drive that is formatted with the FAT32 file system. If you don't have a FAT32 drive, open Disk Management by right-clicking the Start button and choose Disk Management. Click your C partition, right-click and shrink the drive by only 5–10 GBs. Now create a simple volume and format it as FAT32.

Using the `Convert` **Command**

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.

EXERCISE 3.1

Converting a FAT32 Partition to NTFS

1. Copy some folders to the D: drive.

2. Select Start, and 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.

Stopping a Conversion

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 or REGEDT32 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*.

Once you decide which file system you want to use, you need to decide what disk storage type you want to configure. Let's look at some of the disk storage options you have.

> **NOTE** Be careful when converting your file system. Once you change a FAT32 file system to NTFS, you cannot change it back without formatting the disk and losing your data.

Configuring NTFS

As mentioned earlier, NTFS has many advantages over FAT32. The main advantages are NTFS Security, compression, encryption (EFS), and quotas. Let's take a look at some of these advantages in greater detail.

NTFS Security   One of the biggest advantages of NTFS is security. NTFS Security (as shown in Figure 3.1) is one of the most important aspects of an IT administrator's job. An advantage of NTFS Security is that the security can be placed on individual files and folders. It does not matter whether you are local to the share (in front of the machine where the data is stored) or remote to the share (coming across the network to access the data); the security is always in place with NTFS. The default security permission is Users = Read on new folders or shares. Configuring NTFS Security and managing how it works with Shared Permissions are covered in Chapter 4, "Managing Data Access."

FIGURE 3.1   NTFS Security tab
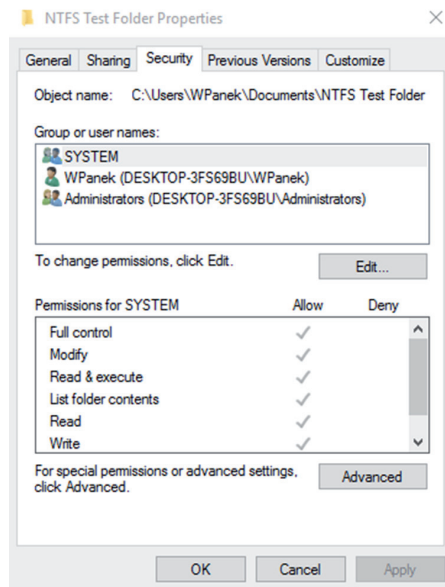
Compression   *Compression* helps compact files or folders to allow for more efficient use of hard drive space. For example, a file that usually takes up 20 MB of space might use only 13 MB after compression. To enable compression, just open the Advanced Attributes dialog box for a folder and check the Compress Contents To Save Disk Space box. Compression is covered in greater detail later in this chapter in the "Managing Data Compression" section.

Encryption   *Encrypting File System (EFS)* allows a user or administrator to secure files or folders by using encryption. Encryption employs the user's security identification (SID) number to secure the file or folder. To implement encryption, open the Advanced Attributes dialog box for a folder, and check the Encrypt Contents To Secure Data box (see Figure 3.2).

FIGURE 3.2   Setting up encryption on a folder
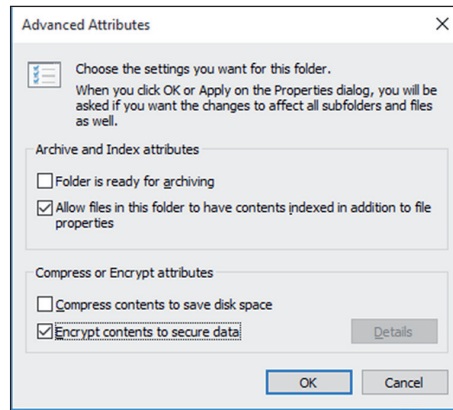
If files are encrypted using EFS and an administrator has to unencrypt the files, there are two ways to do this. First, you can log in using the user's account (the account that encrypted the files) and unencrypt the files. Second, you can become a recovery agent and manually unencrypt the files. EFS is covered in greater detail in the section "Managing Data Encryption with EFS" later in this chapter.

Quotas   Disk *quotas* give administrators the ability to limit how much storage space a user can have on a hard drive. You have a few options available to you when you set up disk quotas. You can set up disk quotas based on volume or on users.

> **Setting Quotas by Volume**   One way to set up disk quotas is by setting the quota by volume, on a per-volume basis. This means that if you have a hard drive with C:, D:, and E: volumes, you would have to set up three individual quotas (one for each volume). This is your umbrella. This is where you set up an entire disk quota based on the volume for all users.

> **Setting Quotas by User**   You have the ability to set up quotas on volumes by user. Here is where you would individually let users have independent quotas that exceed your umbrella quota.

> **Specifying Quota Entries**   You use quota entries to configure the volume and user quotas. You do this on the Quotas tab of the volume's Properties dialog box. (See Exercise 3.2.)

> **Creating Quota Templates**   Quota templates are predefined ways to set up quotas. Templates allow you to set up disk quotas without needing to create a disk quota from scratch. One advantage of using a template is that when you want to set up disk quotas on multiple volumes (C:, D:, and E:) on the same hard drive, you do not need to re-create the quota on each volume.

> Exercise 3.2 will show you how to set up an umbrella quota for all users. This is the disk quota that all users will then follow for whichever drive you set this up on.

EXERCISE 3.2

Configuring Disk Quotas

1. Open Windows Explorer.

2. Right-click the local disk (C:), and choose Properties.

3. Click the Quotas tab.

4. Check the Enable Quota Management check box. Also check the Deny Disk Space To Users Exceeding Quota Limit box.

5. Click the Limit Disk Space To option, and enter **1000MB** in the box.

6. Enter **750MB** in the Set Warning Level To boxes.

7. Click the Apply button. If a warning box appears, click OK. This warning is just informing you that the disk may need to be rescanned for the quota.

8. Now that you have set up an umbrella quota to cover everyone, close the disk quota tool.

Configuring Disk Storage

Windows 10 supports three types of disk storage: basic, dynamic, and GUID Partition Table (GPT). 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 Vista, Windows 7, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 and allows storage to be configured as volumes. GPT support begins with the Windows 2003 SP1 release and allows you to configure volume sizes larger than 2 TB and up to 128 primary partitions. The following sections describe the basic storage, dynamic storage, and GPT storage configurations.

Basic Storage

Basic storage consists of primary and extended partitions and logical drives that exist within the extended partition. The first partition that is created on a hard drive is called a primary partition and is usually represented as the C: drive. Primary partitions use all of the space that is allocated to the partition, and a single drive letter is used to represent the partition. Only a single extended partition is allowed on any basic disk. 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 suballocation of space (called a logical drive) is represented by a different drive letter. For example, a 500 MB extended partition could have a 250 MB D: partition and a 250 MB 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.

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.

Basic storage is the default, and this is the type that many users continue to use. But what if you want some additional functionality from your storage type? Let's look at some of the more advanced disk storage options.

Dynamic Storage

Dynamic storage is a Windows 10 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. Dynamic storage also supports a Redundant Array of Independent Disks (RAID), which will be discussed in the "Understanding RAID" section of this chapter.

To set up dynamic storage, you convert or upgrade a basic disk to a dynamic disk. When converting a basic disk to dynamic, you do not lose any of your data. After the disk is converted, any partitions that existed on the basic disk are converted to dynamic simple volumes, and you can then create any additional dynamic volumes required within the dynamic disk.

You create dynamic storage with the Windows 10 Disk Management utility, which is discussed in the "Using the Disk Management Utility" section of this chapter. Let's take a closer look at the different types of dynamic volumes.

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 3.3 illustrates two simple volumes on a physical disk.

FIGURE 3.3   Two simple volumes

Simple Volume C:\
10 GB

Simple Volume D:\
10 GB

Physical Disk 0
20 GB
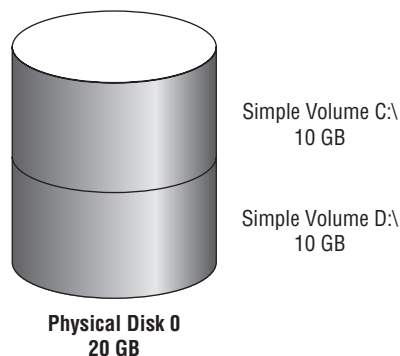
Spanned Volumes

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 or without using another drive letter.

   You do not need to allocate the same amount of space to the volume set on each physical drive. This means you could combine 500 MB on one physical drive with two 750 MB volumes on other dynamic drives, as shown in Figure 3.4.

FIGURE 3.4   A spanned volume set
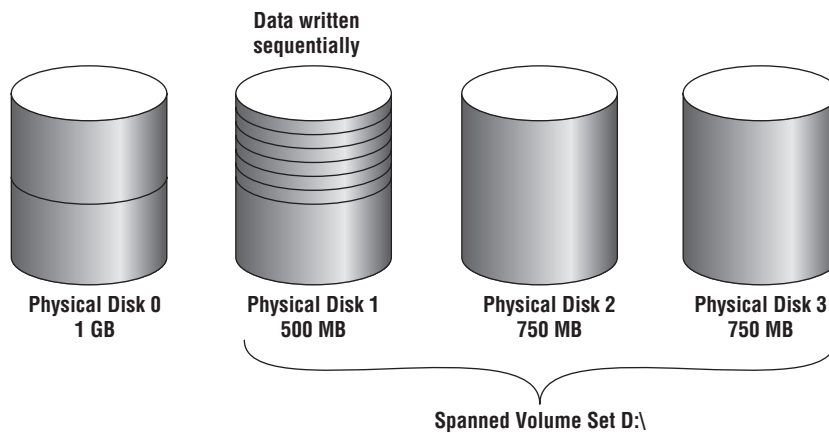
   Because data is written sequentially, you do not see any performance enhancements with spanned volumes as you do with striped volumes (discussed next). The main disadvantage of spanned volumes is that if any drive in the spanned volume set fails, you lose access to all of the data in the spanned set.

Striped Volumes

A *striped volume* stores data in equal stripes between two or more (up to 32) dynamic drives, as illustrated in Figure 3.5. Since the data is written sequentially across the stripe, 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.

FIGURE 3.5   A spanned volume set

Spanned Volume Set D:\
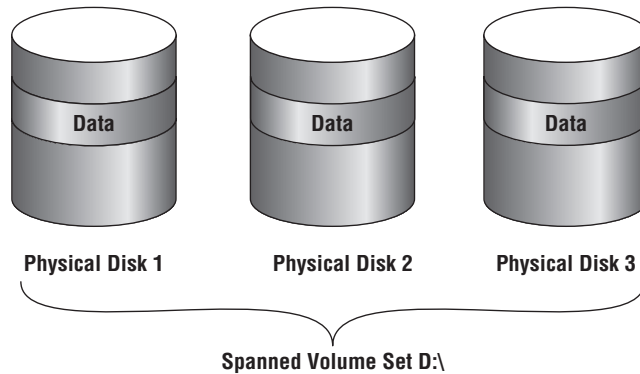
The main disadvantage of striped volumes is that if any drive in the striped volume set fails, you lose access to all of the data in the striped set.

In the last few years a new storage type has emerged in the Microsoft computer world, and as with most new technologies, it has some advantages over the previous technologies. Let's take a look at the newest advantageous storage type.

GUID Partition Table

The *GUID Partition Table (GPT)* is available for Windows 10 and was first introduced as part of the Extensible Firmware Interface (EFI) initiative from Intel. Basic and dynamic disks use the Master Boot Record (MBR) partitioning scheme that all operating systems have been using for years. Basic and dynamic disks use Cylinder-Head-Sector (CHS) addressing with the MBR scheme. CHS allows computers to assign addresses to data on the computer's hard-disk drives. This has been an effective way to store data on a hard drive, but there is a newer, more effective way.

The GPT disk-partitioning system uses the GPT to configure the disk area. GPT uses an addressing scheme called Logical Block Addressing (LBA), which is a newer method of accessing hard-disk drives. LBA uses a unique sector number only instead of using the cylinder, head, and sector number. Another advantage is that the GPT header and partition table are written to both the front and back ends of the disk, which provides for better redundancy.

The GPT disk-partitioning system gives you many benefits over using the MBR system:

- Allows a volume size larger than 2 TB
- Allows up to 128 primary partitions
- Used for both 32-bit and 64-bit Windows 10 editions
- Includes cyclic redundancy check (CRC) for greater reliability

However, there is one disadvantage to using the GPT drives. You can convert a GPT drive only if the disk is empty and unpartitioned. I will show you the steps to creating a GPT disk later in this chapter.

To convert any disk or format any volume or partition, you can use the Disk Management utility. I will show you how to manage your disks using the Disk Management utility in the "Using the Disk Management Utility" section, later in this chapter.

Cloud-Based Storage

One of the fastest-growing parts of the IT world is cloud-based services. From cloud-based user storage to cloud-based corporate data storage, it seems like all we hear anymore is "cloud, cloud, cloud."

Well, Microsoft has cloud-based subscription services called Microsoft Azure and OneDrive.

Microsoft Azure

Microsoft Azure (`https://azure.microsoft.com/en-us/`) can be used by almost any operating system on the market (Windows, Linux, etc.), by most applications (Java, .NET, PHP, etc.), and by most device types (Windows, Android, and iOS).

Microsoft Azure is different than many other cloud-based systems because Microsoft Azure doesn't make you choose either your network or the cloud. Many cloud-based service providers want you to use their cloud to run all of your applications and/or storage from their location. Microsoft Azure allows you to extend your current network infrastructure into the cloud to take full advantage of both worlds.

This way you can still have a full IT server room with full-time IT employees but get the benefits of storing data both locally and also in a cloud environment, which is then available from anywhere in the world.

Azure makes it easy to store documents in the cloud by using the Azure portal. The portal is the way that users and IT professionals can control and manage how data is stored in the cloud. The Azure portal allows you to do some of the following:

- Upload and download data to and from Azure

- Run reports showing the actual usage of each file share

- Adjust the quota sizes of your users

- Use the `net use` command-line utility to share files from a Windows client command prompt

One advantage to using Microsoft Azure is that you only pay for what you need. The more cloud-based storage you need, the more you pay for and the less you need means less money. Table 3.2 shows you the maximum amount of data that can be stored on Microsoft Azure.

TABLE 3.2   Microsoft Azure data size availability

Operating System	Maximum Size of Data Source
Windows Server 2012 or above	54,400 GB
Windows 8 or above	54,400 GB

TABLE 3.2   Microsoft Azure data size availability *(continued)*

Operating System	Maximum Size of Data Source
Windows Server 2008, Windows Server 2008 R2	1,700 GB
Windows 7	1,700 GB

If you decide that you want your company to use Microsoft Azure for some of its cloud-based storage or all of its cloud-based storage, please go to `https://azure.microsoft.com/en-us/` to get the current subscription rates.

Microsoft OneDrive

Another Microsoft-based subscription is called OneDrive (used to be known as SkyDrive). Microsoft's OneDrive is built into Windows 10 by default (see Figure 3.6). OneDrive is a cloud-based storage subscription so home users can store their documents and then access those documents from anywhere in the world (provided that you have Internet access).

FIGURE 3.6   OneDrive welcome screen
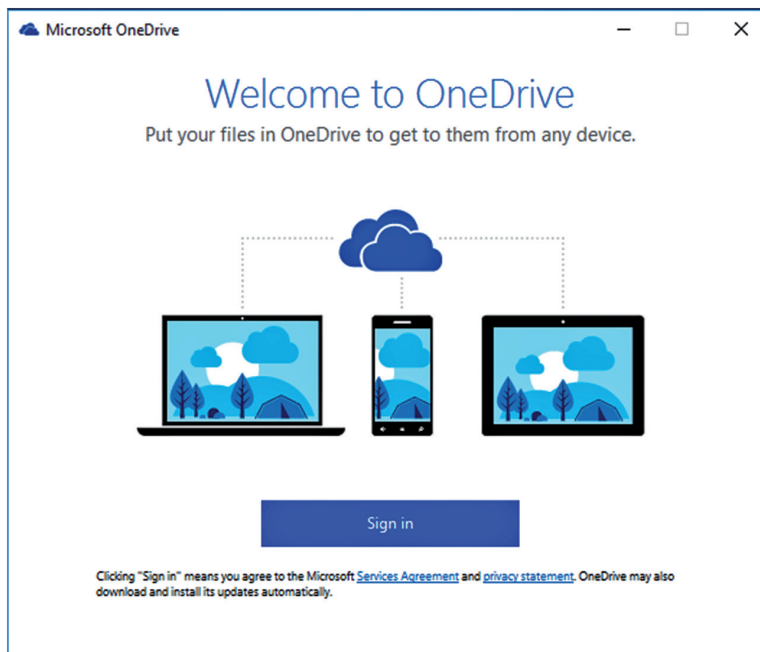
OneDrive was designed for the average home user who is looking to store data in a safe, secure, cloud-based environment. OneDrive, when first released, was also a consideration for corporate environments, but with the release of Windows Azure, OneDrive is really intended for the home user or corporate user who wants to store some of their own personal documents in the cloud. Corporations would be more inclined to use Microsoft Azure and all of its corporate benefits.

If you or your company decides to purchase the Office 365 subscription, then OneDrive is included for cloud-based storage. If you didn't purchase Office 365, then you have to choose from one of the subscriptions shown in Table 3.3.

TABLE 3.3 OneDrive Subscriptions

Amount of Storage	Subscription Monthly Fee
Office 365 + 1 TB included	$9.99
5 GB	Free
100 GB	$1.99
200 GB	$3.99

Please note that these are the current prices at the time this book was written and these prices may have changed. Be sure to check out Microsoft's OneDrive web page for current prices (`https://onedrive.live.com/options/Upgrade`).

Exercise 3.3 will show you how to set up a OneDrive account for your user account. To do this access, you must have a Microsoft account. You get 15 GB for free from Microsoft on the OneDrive cloud-based storage.

EXERCISE 3.3

Configuring OneDrive

1. Open OneDrive.
2. Log into OneDrive using your Microsoft account as shown in Figure 3.7.

FIGURE 3.7   OneDrive login screen
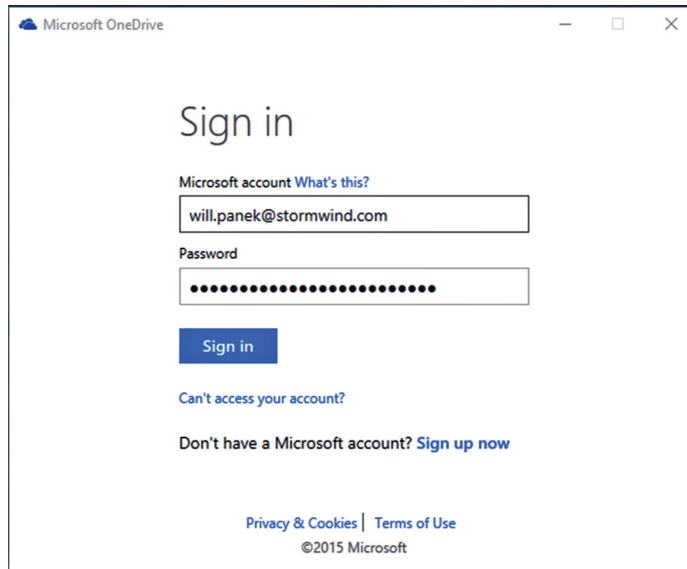
3.   You will get a screen that will show you where your files will be located on your system as shown in Figure 3.8. Click the Next button.

FIGURE 3.8   OneDrive file location screen
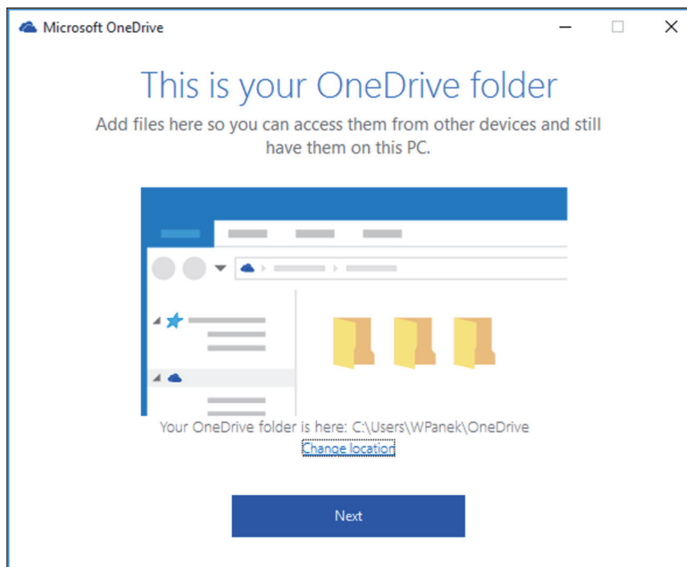
4. At the Sync files screen, choose what folders that you want to sync with Microsoft and then click Next.

    A screen will appear telling you that your OneDrive is set up and ready to go (see Figure 3.9).

    FIGURE 3.9   Open My OneDrive Folder screen
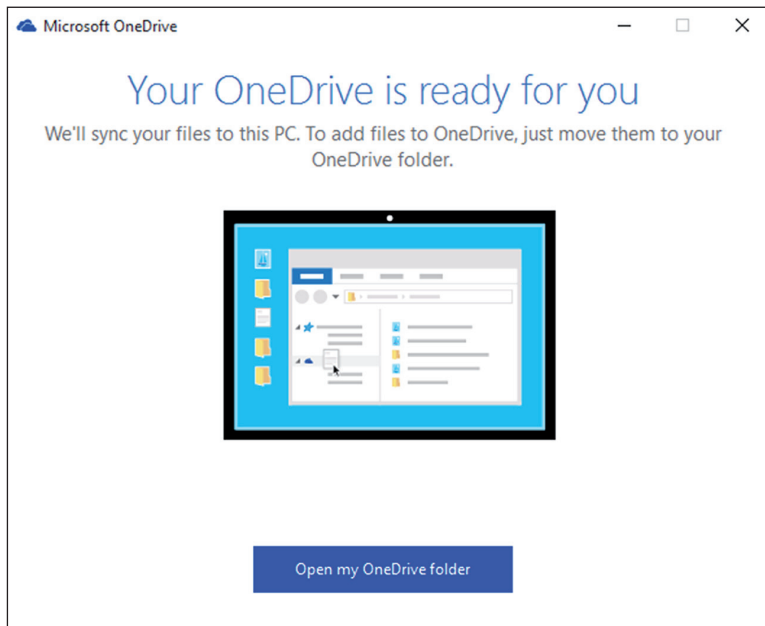
5. Click the Open My OneDrive Folder button to open your folders and Microsoft OneDrive.

6. Close OneDrive.

> **NOTE**   Cloud-based services will be discussed throughout this book.

Using the Disk Management Utility

The Disk Management utility is a Microsoft Management Console (MMC) snap-in that gives administrators a graphical tool for managing disks and volumes within Windows 10. In this section, you will learn how to access the Disk Management utility and use it to perform basic

tasks, including managing basic storage, and dynamic storage. You will also learn about troubleshooting disks through disk status codes.

But before we dive into the Disk Management utility, let's explore the MMC. It is important to understand the MMC since Disk Management (like many other tools) is actually an MMC snap-in.

Using the Microsoft Management Console

The *Microsoft Management Console (MMC)* is the console framework for application management. The MMC provides a common environment for snap-ins. Snap-ins are administrative tools developed by Microsoft or third-party vendors. Some of the MMC snap-ins that you may use are Computer Management, Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and DNS Management. When you look at the administrative tools, you know that each one of these tools are running inside of an MMC (shown in Figure 3.10).

F I G U R E   3 . 1 0   The administrative tools running in MMCs
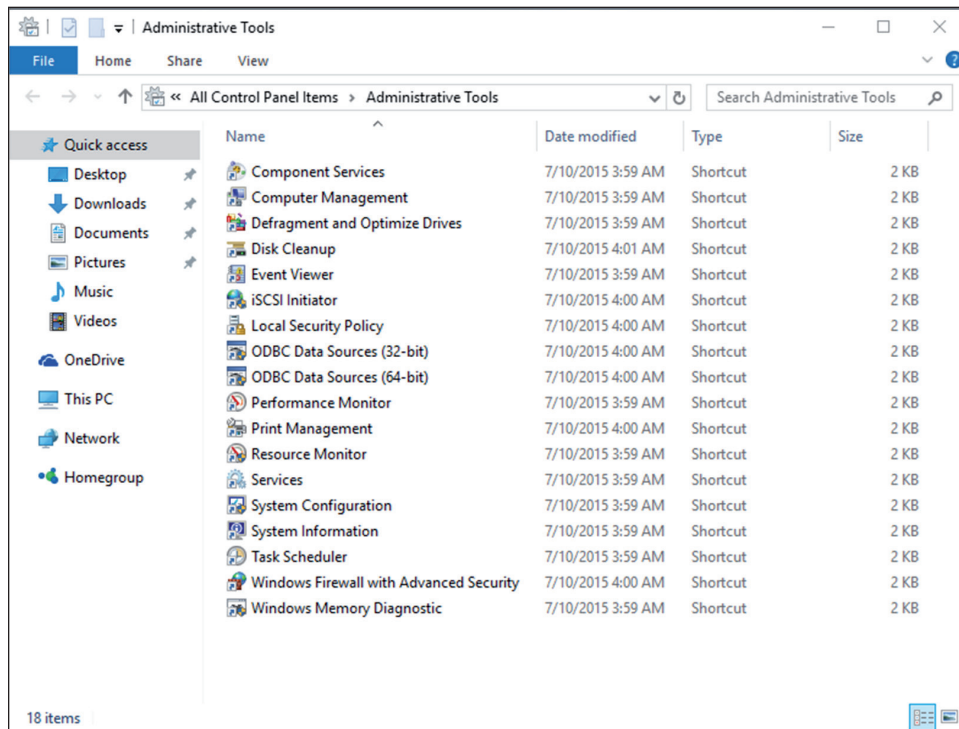
Knowing how to use and configure the MMC snap-ins will allow you to customize your work environment. For example, if you are in charge of Active Directory Users and Computers

and DNS, you can add both of these snap-ins into the same window. This would then allow you to open just one application to configure all your tasks. The MMC offers many other benefits:

- 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 customized MMCs and share them 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 3.11, by default, the MMC 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.

FIGURE 3.11   The MMC tree, details pane, and Actions pane
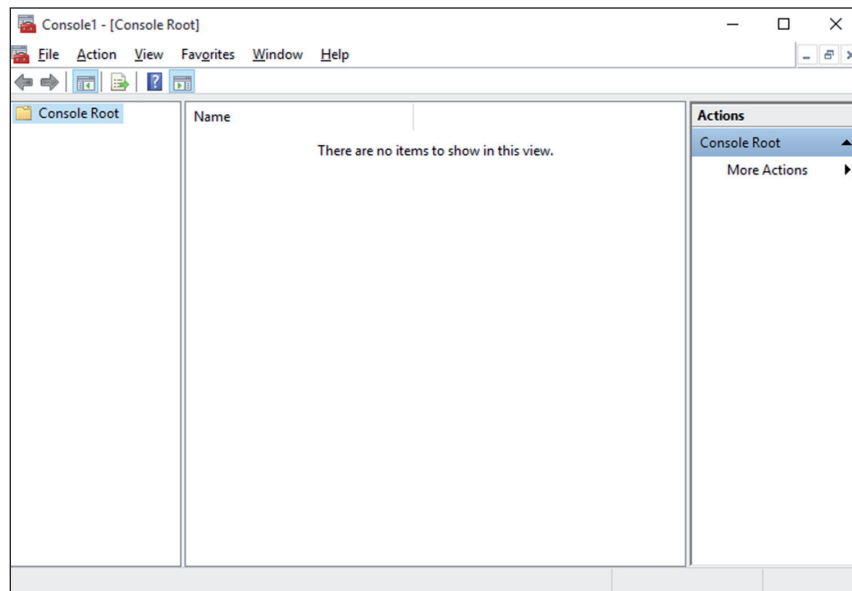
To open the MMC on a Windows 10 computer, click the Start button and type **MMC** in the Search dialog box. When you first open the MMC, it contains only the `Console Root` folder, as shown in Figure 3.11. The MMC does not have any default administrative functionality. It is simply a framework used to organize administrative tools through the addition of snap-in utilities.

The first thing that you should decide when using the MMC is which of the different administrative mode types you will employ. You need to decide which mode type is best suited to use for your organization.

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, while in the MMC editor, select File ➢ Options to open the Options dialog box. In this dialog box, you can select from the console modes listed in Table 3.4.

TABLE 3.4   MMC modes

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

After you decide which administrative role you are going to run, it's time to start configuring your MMC snap-ins.

Adding Snap-Ins

The biggest advantage of using the MMC is to configure snap-ins the way your organization needs them. Adding snap-ins is a simple and quick procedure. To add a snap-in to the MMC and save it, complete Exercise 3.4.

EXERCISE 3.4

Adding an MMC Snap-In

1. To start the MMC editor, click Start, type **MMC** into the search box, and press Enter.

2. From the main console window, select File ➢ Add/Remove Snap-In to open the Add Or Remove Snap-ins dialog box.

3. Highlight the snap-in you want to add (see Figure 3.12), and click the Add button.

FIGURE 3.12   The MMC Add Or Remove Snap-Ins screen
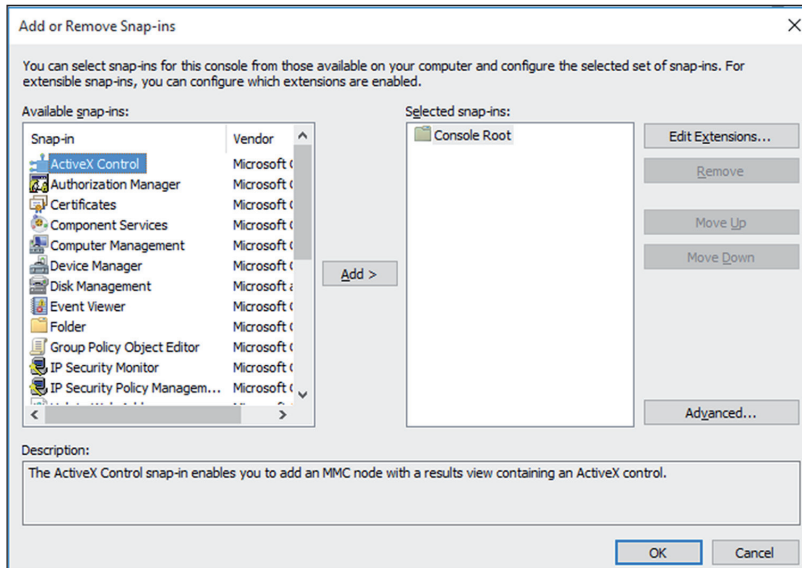
4. If prompted, specify whether the snap-in will be used to manage the local computer or a remote computer. After you choose the MMCs you want in your custom snap-in (shown in Figure 3.13), click the Finish button.

FIGURE 3.13   The MMC console screen
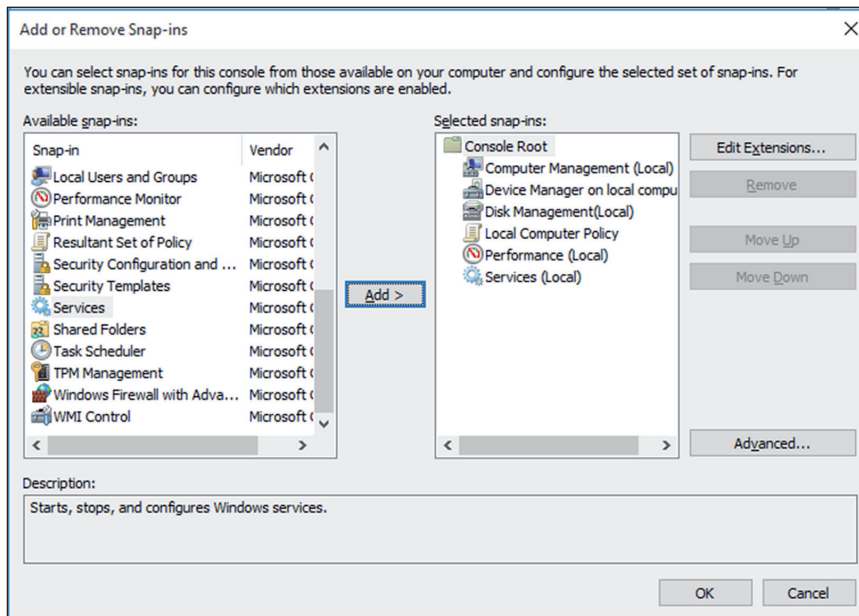
5. When you have finished adding snap-ins, click OK.

6. 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. Place the console on the desktop as shown in Figure 3.14.

FIGURE 3.14   The MMC console on desktop
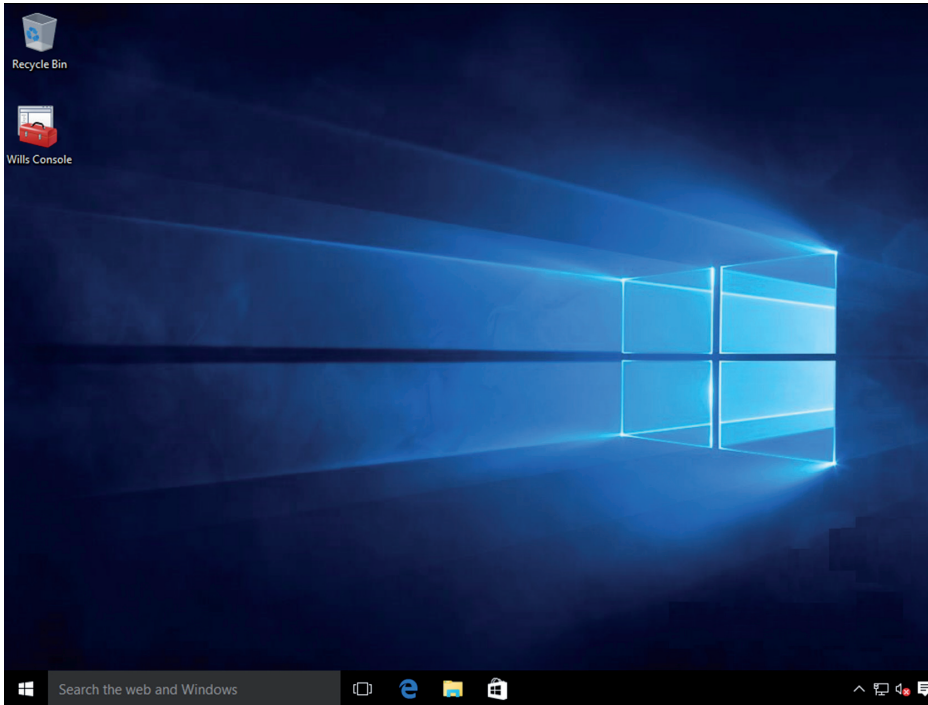
You can save the console to a variety of locations, including a program group or the desktop. By default, custom consoles have an `.msc` filename extension.

Many applications that are MMC snap-ins, including Disk Management, are already configured for you under the Administrative Tools section of Windows 10. Next, let's look at the Disk Management utility.

Understanding the Disk Management Utility

The Disk Management utility, located under the Computer Management snap-in by default, is a one-stop shop for configuring your disk options.

First of all, to have full permissions to use the Disk Management utility, you must be logged on with local Administrative privileges. You can access the Disk Management utility a few different ways. You can right-click Computer from the Start menu and select Manage, and then in Computer Management, select Disk Management. You could also use Control Panel ➢ Administrative Tools ➢ Computer Management.
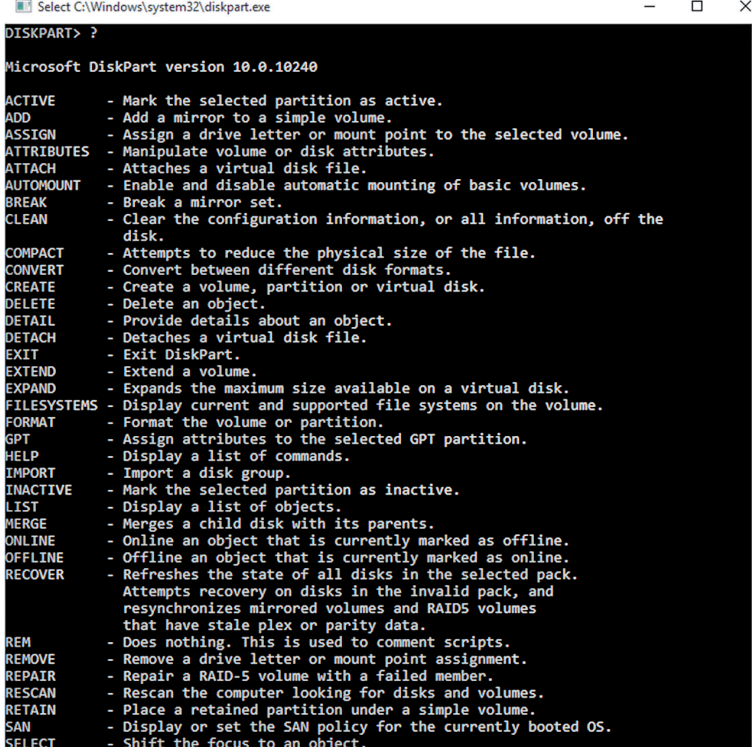
Once you have launched Computer Management, you must expand the storage section of the console in order to access the Disk Management toolset. The Disk Management utility's opening window, shown in Figure 3.15, displays the following information:

- 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

FIGURE 3.15   The Disk Management window
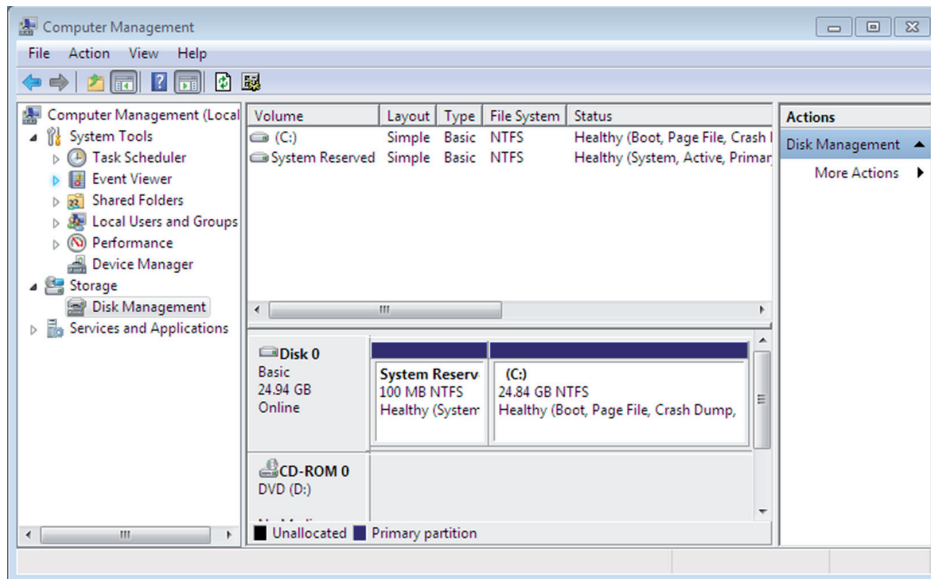
Windows 10 also includes a command-line utility called Diskpart, which can be used as a command-line alternative to the Disk Management utility. You can view all of the options associated with the Diskpart utility by typing **Diskpart** (as shown in Figure 3.16) at a command prompt and then typing **?** at the Diskpart prompt.

FIGURE 3.16   The Diskpart window

The Disk Management utility allows you to configure and manage your disks. Let's take a look at some of the tasks that you can perform in disk administration.

Managing Administrative Hard-Disk Tasks

The Disk Management utility allows you to perform a variety of hard-drive administrative tasks:

- View disk properties.
- View volume and local disk properties.
- Add a new disk.
- Create partitions and volumes.
- Upgrade a basic disk to a dynamic or GPT disk.
- Change a drive letter and path.
- Resize a volume or partition.
- Delete partitions and volumes.

These tasks are discussed in the sections that follow.

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 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 3.17, 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 partition style
- The capacity of the disk
- The amount of unallocated space on the disk
- The amount of space reserved on the disk
- The logical volumes that have been defined on the physical drive

FIGURE 3.17   The Volumes tab of a disk's Properties dialog box
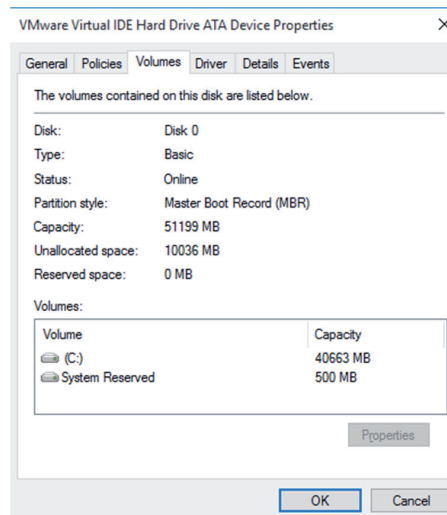
If you click the General tab of a disk's Properties dialog box, the hardware device type, the hardware vendor that produced the drive, the physical location of the drive, and the device status are displayed.

Viewing Volume and Local Disk Properties

On a dynamic disk, you manage volume properties. On a basic disk, you manage partition properties. Volumes and partitions 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 partition 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 seven tabs: General, Tools, Hardware, Sharing, Security, Previous Versions, and Quota. The Security tab and Quota tab appear only for NTFS volumes. All these tabs are described in detail in the following text.

General　The information on the General tab of the volume's Properties dialog box, as shown in Figure 3.18, 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.

FIGURE 3.18　General properties for a volume
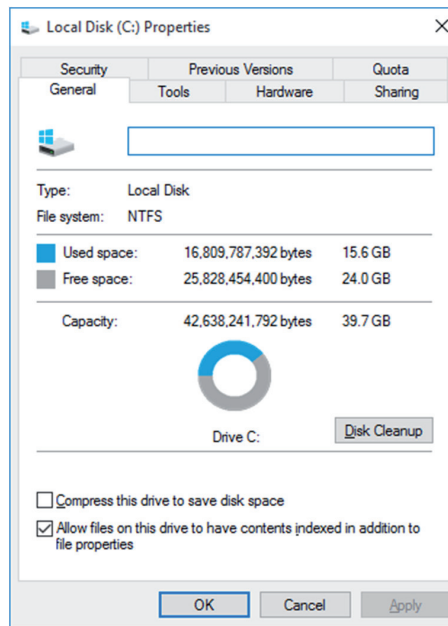
The label on a volume or local disk is for informational purposes only. For example, depending on its use, you might give a volume a label such as APPS or ACCTDB.

The Disk Cleanup button starts the Disk Cleanup utility, which you can use to delete unnecessary files, thereby freeing 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.

Tools   The Tools tab of the volume's Properties dialog box, shown in Figure 3.19, provides access to three tools.

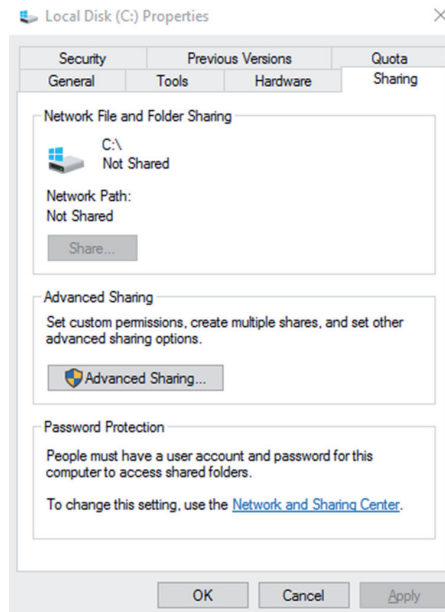**FIGURE 3.19**   The Tools tab of the volume's Properties dialog box
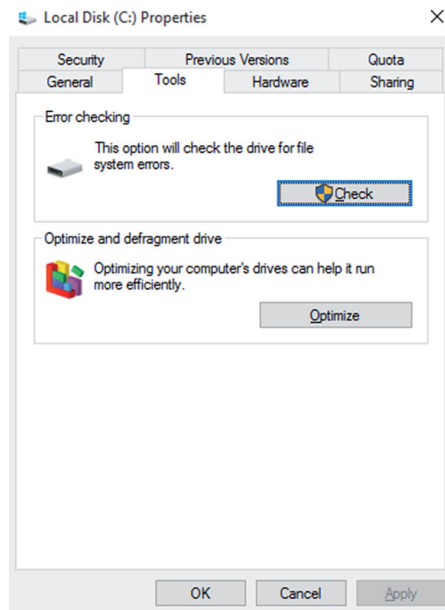
Click the Check Now button to run the Error-Checking utility to check the volume for errors. You may do this if you are experiencing problems accessing the volume or if the volume was open during a system restart that did not go through a proper shutdown sequence. This utility is covered in more detail in "Troubleshooting Disk Management," later in this chapter.

Click the Optimize Now button to run the Disk Defragmenter utility. This utility defragments files on the volume by storing the files contiguously on the hard drive.

Hardware   The Hardware tab of the volume's Properties dialog box, shown in Figure 3.20, lists the hardware associated with the disk drives that are recognized by the Windows 10 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.

FIGURE 3.20 The Hardware tab of the volume's Properties dialog box
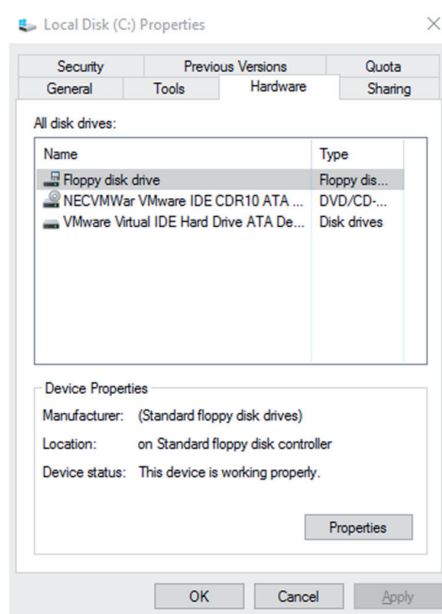
For more details about a hardware item, highlight it and click the Properties button in the lower-right corner of the dialog box. This brings up a Properties dialog box for the item. Your Device Status field should report, "This device is working properly." If that's not the case, you can click the Troubleshoot button (it will appear if the device is not working properly) to get a troubleshooting wizard that will help you discover the problem.

Sharing   On the Sharing tab of the volume's Properties dialog box, shown in Figure 3.21, you can specify whether or not the volume is shared on the network. Volumes are not shared by default. Clicking the Advanced Sharing button 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.

Security   The Security tab of the volume's Properties dialog box, shown in Figure 3.22, 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 3.23. Shadow copies of files are backup copies created by Windows in the background 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.

FIGURE 3.21   The Sharing tab of the volume's Properties dialog box

FIGURE 3.22   The Security tab of the volume's Properties dialog box
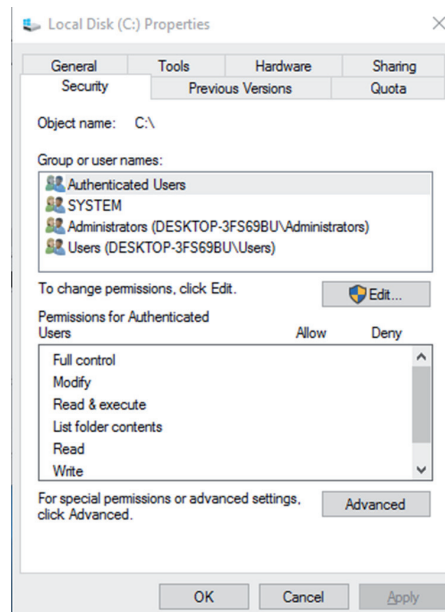
FIGURE 3.23 The Previous Versions tab of the volume's Properties dialog box
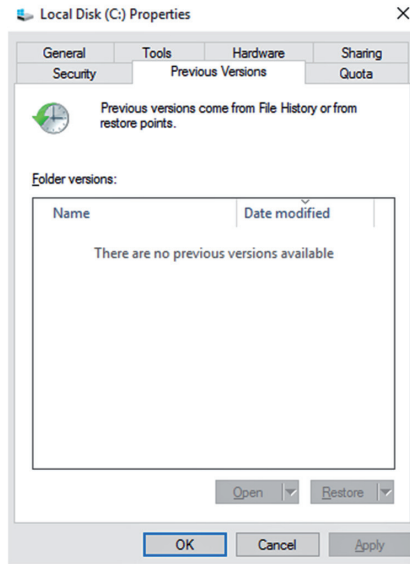
Quota Quotas give you the ability to limit the amount of hard-disk space that a user can have on a volume or partition (see Figure 3.24). By default, quotas are disabled. To enable quotas, check the Enable Quota Management check box. There are a few options that can be configured when enabling quotas.

FIGURE 3.24 The Quota tab of the volume's Properties dialog box
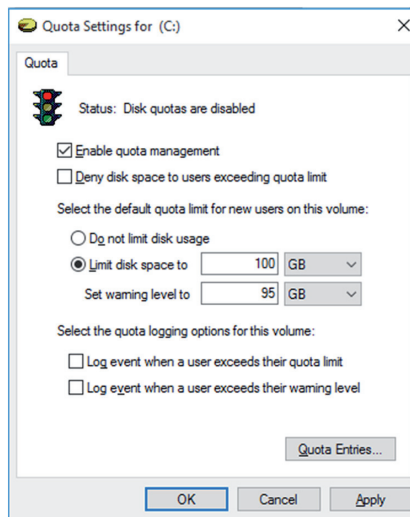
The Deny Disk Space To Users Exceeding Quota Limit check box is another option. When this box is enabled, any user who exceeds their quota limit will be denied disk storage. You can choose not to enable this option, which allows you to just monitor the quotas. You also have the ability to set the quota limit and warning size and to log all quota events as they happen.

Adding a New Disk

New hard disks can be added to a system 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. Remember, your user account must be a member of the Administrators group to install a new drive. The following list specifies configuration options:

Computer Doesn't Support Hot Swapping   If your computer does not support hot swapping, you must 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.

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

Creating a volume or partition is a fairly easy process. To create the new volume or partition, right-click the unformatted free space and start the wizard.

Exercise 3.5 walks you through the New Volume Wizard for creating a new volume.

EXERCISE 3.5

Creating a New Volume

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 be able to create only 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. Select the size of volume to create, and then click Next to continue.

4. You should see the Assign Drive Letter Or Path screen. 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 into an empty folder, you can have a virtually unlimited number of volumes, negating the drive-letter limitation. If you choose not to assign a drive letter or path, users will not be able to access the volume. Make your selections, and click Next to continue (see Figure 3.25).

FIGURE 3.25 Assign Drive Letter Or Path screen
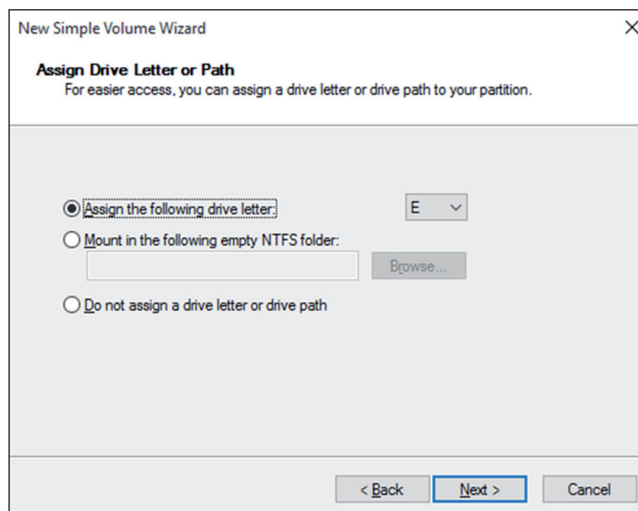
5. The Format Partition screen appears. This screen allows you to choose whether you will format the volume. If you choose to format the volume, you can format it as FAT32 or NTFS. You can also select the allocation unit size, enter a volume label (for information only), specify whether you would like to perform a quick format, and choose whether to enable file and folder compression. After you've made your choices, click Next (see Figure 3.26).

FIGURE 3.26   Format Partition screen
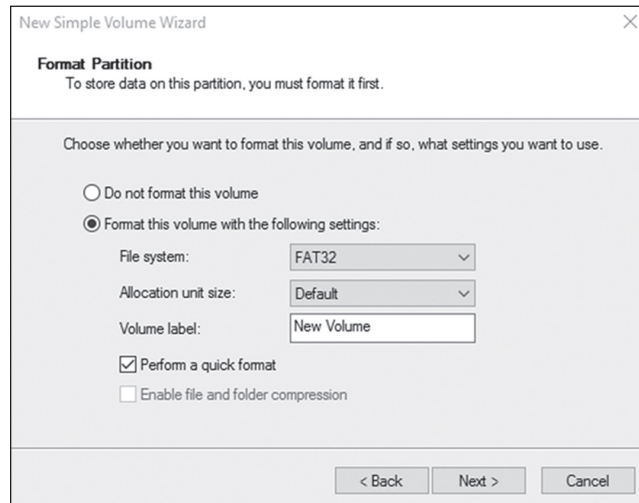
6.   The Completing The New Volume Wizard screen appears. Verify your selections. If you need to change any of them, click the Back button to reach the appropriate screen. When everything is correctly set, click the Finish button.

Now that you know how to create a new volume or partition, let's see how to convert a basic disk to dynamic or GPT.

Upgrading a Basic Disk to a Dynamic or GPT Disk

When you perform a fresh installation of Windows 10, your drives are configured as basic disks. To take advantage of the features offered by Windows 10 dynamic or GPT disks, you must upgrade your basic disks to either of those disk configurations.

> **WARNING**   Upgrading basic disks to dynamic disks is a one-way process as far as preserving data is concerned and is 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 before proceeding with the change.

Any basic disk can be converted to a dynamic disk, but only a disk with all unformatted free space can be converted to a GPT disk. Exercise 3.6 walks you through converting an MBR-based disk to a GPT disk.

Converting a Basic Disk to a GPT Disk

1. If the disk that you want to convert has partitions or volumes defined, first delete the partition or volume.

2. Open the Disk Management utility by clicking the Start button, right-clicking Computers, and choosing Manage.

3. Click Disk Management in the lower-left section.

4. Right-click the disk and choose Convert To GPT Disk (see Figure 3.27).

FIGURE 3.27 Format Partition Screen
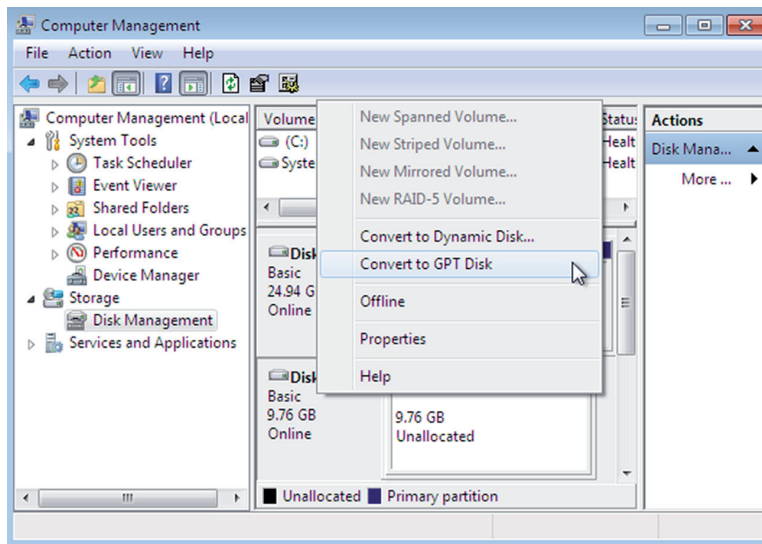
5. After the disk converts, you can right-click the disk and see that the Convert To MBR Disk option is now available.

NOTE There are a few other methods for converting an MBR-based disk to a GPT disk. You can use the Diskpart utility and type in the `Convert GPT` command. You can also create a GPT disk when you first install a new hard drive. After you install the new hard drive, during the initialization phase, you can choose GPT Disk.

Another type of conversion that you may need to perform is that from a basic disk to a dynamic disk. Complete Exercise 3.7 to convert a basic disk to a dynamic disk.

EXERCISE 3.7

Converting a Basic Disk to a Dynamic Disk

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 convert 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.

As you are configuring the volumes or partitions on the hard drive, other things that you may need to configure are the drive letters and paths.

Changing the Drive Letters and Paths

There may be times when you need to change drive letters and paths when you add new equipment. Let's suppose you have a hard drive with two partitions: drive C: assigned as your first partition and drive D: assigned as your second partition. Your DVD drive is assigned the drive letter E:. You add a new hard drive and partition it as a new volume. By default, the new partition is assigned as drive F:. If you want your logical drives to be listed before the DVD drive, you can use the Disk Management utility's Change Drive Letter And Paths option to reassign 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 3.28. Click the Change button to access the Change Drive Letter Or Path dialog box shown in Figure 3.28. 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.

FIGURE 3.28   The dialog boxes for changing a drive letter or path
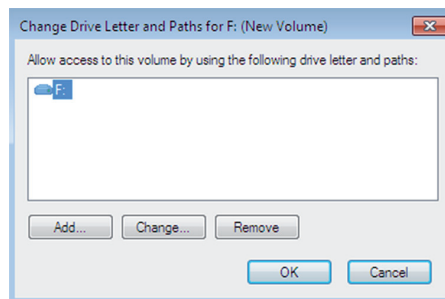
In Exercise 3.8, you will edit the drive letter of the partition you created.

EXERCISE 3.8

Editing a Drive Letter

1. Right-click Start ➢ Computer Management; then expand Storage ➢ Disk Management.

2. Right-click a drive that you have created 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.

Another activity that you may need to perform is deleting a partition or volume that you have created. The next section looks at these activities.

Deleting Partitions and Volumes

When configuring your hard disks, there may be a time that you want to reconfigure your drive by deleting the partitions or volumes on the hard drive. You may also want to delete a volume so that you can extend another volume. These are tasks that can be configured in Disk Management.

When deleting a volume or partition, you will see a warning that all the data on the partition or volume will be lost. You have to click Yes to confirm that you want to delete the volume or partition. This confirmation is important because once you delete a partition or volume, it's gone for good along with any data content that was contained within it.

> **NOTE**   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 10, you can use a third-party disk-management utility.

In Exercise 3.9, you will delete a partition that you have created. Make sure that if you delete a partition or volume, it is empty; otherwise, back up all the data that you would like to retain before the deletion.

EXERCISE 3.9

Deleting a Partition

1. In the Disk Management utility, right-click the volume or partition that you want to remove and choose Delete Volume.

2. A warning box appears, stating that once this volume is deleted, all data will be lost. Click Yes.

3. The volume will be removed, and the area will be returned as unformatted free space.

You may be worried about your users removing devices from their Windows 10 machines. Microsoft has helped you in this situation. You can use removable-device policies to help restrict your users from removing their hardware. Removable-device policies can be created through the use of a Group Policy Object (GPO) on the server. GPOs are policies that are set on a computer or user and allow you to manipulate the Windows 10 environment.

Now that we have explored some of the basic administrative tasks of Disk Management, let's look at how to manage storage.

Managing Storage

The Disk Management utility offers support for managing storage. You can create, delete, and format partitions or volumes on your hard drives. You can also extend or shrink volumes on dynamic disks. Additionally, you can delete volume sets and striped sets.

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, you use the New Volume Wizard to create a new volume. To start the New Volume 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 2 to 32 drives into a single logical partition. The free space on all drives must be equal in size in a striped volume. Data in the striped volume is written across all drives in 64 KB stripes. (Data in spanned and extended volumes is written sequentially.) Striped volumes offer you better performance and are normally used for temporary files or folders. The problem with a striped volume is if you lose one of the drives in the volume, the entire striped volume is lost.

Another option that you have with volumes is to extend the volumes to create a larger storage area. In the next section, we will look at that process.

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 is created when you are using only one physical drive. A spanned volume is created when you are using two or more physical drives. Exercise 3.10 shows you how to create an extended volume.

EXERCISE 3.10

Creating 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 3.29, 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.

FIGURE 3.29   The Select Disks screen
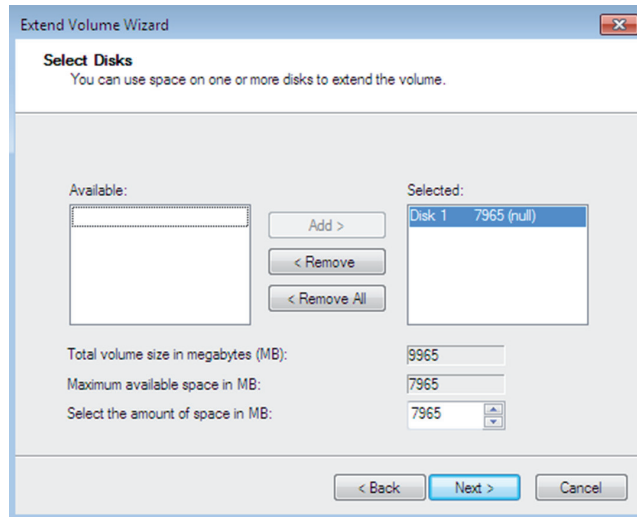
4. The Completing The Extend Volume Wizard screen appears. Click the Finish button. You will see the new volume.

Once a volume is extended, no portion of it can be deleted without losing data on the entire set. However, if there is unneeded space on a volume, you can shrink that volume without losing data by using the Shrink Volume option in Disk Management.

🌐 Real World Scenario

You're Running Out of Disk Space

Crystal, 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. Crystal has a 250 GB 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 because it must be stored on a single drive letter. Crystal's computer has a single SATA drive with nothing attached to the second SATA channel.

You have two basic options for managing space in this circumstance. 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 Crystal 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 Crystal's workload allows time for maintenance, you can replace the volume set with a single drive.

One issue you may run into with hard drives is that they go bad from time to time. If you have ever heard a hard drive fail, you know the sound: it is a distinct clicking. Once you have experienced it, you will never forget it. When drives go bad, Disk Management can help determine which drive and what the issue may be. Next, we will look at hard-disk errors.

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.

The problem with disk errors is that you don't know when a disk fails or which disk failed. Disk Management can help you with this. When disks have problems or errors,

status codes get assigned. Knowing what these codes mean will help you determine what the problem is and, more important, what steps need to be taken to fix the problem.

Understanding 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)   Used only with dynamic disks, this code 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, this code 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 reaccess 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. It 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   This can be seen with basic or dynamic volumes. It 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. It 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, the data will be inaccessible.

Foreign   This error can occur if you move a dynamic disk from a computer running Windows 2000 (any version), Windows Server 2003, Windows 2008, Windows Server

2008 R2, Windows Server 2012/2012 R2, Windows XP Professional, Windows 7, Windows Vista, or Windows 8.1 to a Windows 10 computer. This error occurs 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 Import Foreign Disks option. Any existing volume information will then be visible and accessible.

In addition to errors, there are some other issues that can arise when installing or configuring disks. One issue that may occur is that a disk fails to initialize when installed.

Troubleshooting Disks That Fail to Initialize

When you add a new disk to your computer in Windows 10, 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.

As you have now seen, Disk Management can be a very useful tool in your computer management arsenal. If you decide to format your partition or volume using NTFS, you then receive added benefits like compression, encryption (and therefore security), and quotas. In the following sections, we will take a closer look at compression and encryption.

Managing Data Compression

One of the advantages of using NTFS over FAT32 is the ability to compress data. I teach IT Administrators data compression, and I like to refer to a well-known infomercial as an example. Have you seen the commercial where people put all of the blankets into a large bag and then hook a vacuum to the bag and suck all the air out? This is a great example of how compression works. Data compression is the process of storing data in a form that takes less space than uncompressed data.

If you have ever "zipped" or "packed" a file, you have used a form of data compression. The compression algorithms support cluster sizes only up to 4 KB, 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.

The following are some important points about compression:

- Files as well as folders in NTFS can be compressed and 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.

- Compression happens very quickly, but if, for example, you compress a 500 GB hard drive, there is no guarantee that there won't be any lag time on your machine or server.

- Data compression is available only on NTFS partitions. Because of this, if you copy or move a compressed folder or file to a FAT32 partition, Windows 10 automatically uncompresses the folder or file.

- Certain system files (e.g., Pagefile.sys) can't be compressed.

- You have the ability to show compressed files and folders with an alternate color.

In Exercise 3.11, you will compress and uncompress folders and files.

EXERCISE 3.11

Compressing and Uncompressing Folders

1. Select Start ➢ Run, and then type **Explorer** and click OK.

2. In Windows Explorer, find and select Computer, Local Disk (C:), and then a folder on the C: 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 (see Figure 3.30). Then click OK.

   FIGURE 3.30 The Advanced Attributes dialog box
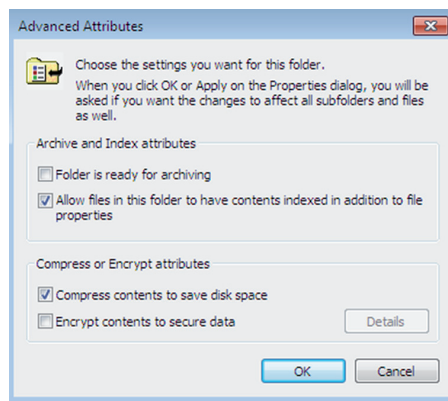
5. In the Confirm Attribute Changes dialog box, select the option Apply Changes To This Folder, Subfolders and Files. (If this confirmation dialog box does not appear, you can

display it by clicking the Apply button in the Properties dialog box.) Click OK to con-firm 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 in Exercise 3.11 and uncheck the Compress Contents To Save Disk Space option in the Advanced Attributes dialog box.

As I stated earlier, you can specify that compressed files be displayed in a different color from uncompressed files. To do so, in Windows Explorer select View ➢ Options. In the Options box, click the View tab and under Files And Folders, check the Show Encrypted Or Compressed NTFS Files In Color option.

In addition to compressing files and folders in Windows Explorer, you can compress the files and folders using the Compact command-line utility.

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. 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). Some of the options that can be used with the Compact command are shown in Table 3.5.

TABLE 3.5   Compact commands

Command	Description
/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 been hidden or system file attributes
/I	Indicates that errors should be ignored
/F	Forces a file to be compressed
/Q	Used with reporting, to report only critical information
/?	Displays help

Another way that you can save disk space is by zipping folders. In the following section, we will discuss how to save space using zipped folders.

Using Compressed (Zipped) Folders

Windows 10 also supports compressed (zipped) folders. This feature is different from NTFS compressed folders. The advantage of using compressed (zipped) folders is that they are supported on FAT32 and NTFS volumes. In addition, you can use compressed (zipped) folders to share data with other programs that use zipped files. The downside to using compressed (zipped) folders is that it is slower than using NTFS compression.

Within Windows Explorer, you create a zipped folder (or file) by right-clicking the folder and selecting Send To ➤ Compressed (Zipped) Folder. You create a zipped file by right-clicking a file and selecting New ➤ Compressed (Zipped) Folder. When you create a compressed folder, it will be displayed as a folder with a zipper.

Understanding Distributed File System

One problem that network administrators have is deciding how to share folders and communicating to the end users how to find the shares. For example, if you share a folder called `Stormwind Documents` on server A, how do you make sure that your users will find the folder and the files within it? The users have to know the server name and the share name. This can be a huge problem if you have hundreds of shares on multiple servers. If you want to have multiple copies of the folder called `Stormwind Documents` for fault tolerance and load balancing, the problem becomes even more complicated.

Distributed File System (DFS) in Windows Server 2012 R2 offers a simplified way for users to access geographically dispersed files. DFS allows you to set up a tree structure of virtual directories that allow users to connect to shared folders throughout the entire network.

Administrators have the ability to take shared folders that are located on different servers and transparently connect them to one or more DFS namespaces—virtual trees of shared folders throughout an organization. The advantage of using DFS is that if one of the folders becomes unavailable, DFS has failover capability that will allow your users to connect to the data on a different server.

Administrators can use the DFS tools to choose which shared folders will appear in the namespace and also to decide how the names of these shared folders will show up in the virtual tree listing. Administrators can then deploy the DFS shared folders to the Windows 10 DFS clients.

Advantages of DFS

One of the advantages of DFS is that when a user views this virtual tree, the shared folders appear to be located on a single machine. The following list includes some other advantages of DFS:

Simplified Data Migration   DFS gives you the ability to move data from one location to another without the user needing to know the physical location of the data. Because the users do not need to know the physical location of the shared data, administrators can simply move data from one location to another.

Security Integration   Administrators do not need to configure additional security for the DFS shared folders. The shared folders use the NTFS and shared folder permissions that an administrator has already assigned when the share was set up.

Access-Based Enumeration (ABE)   This DFS feature (disabled by default) displays only the files and folders that a user has permissions to access. If a user does not have access to a folder, Windows hides the folder from the user's DFS view. This feature is not active if the user is viewing the files and folders locally.

Types of DFS

The following are types of DFS:

DFS Replication   Administrators have the ability to manage replication scheduling and bandwidth throttling using the DFS management console. Replication is the process of sharing data between multiple machines. As explained earlier in the section, replicated shared folders allow you to balance the load and have fault tolerance. DFS also has read-only replication folders.

DFS Namespaces   The DFS Namespace service is the virtual tree listing in the DFS server. An administrator can set up multiple namespaces on the DFS, allowing for multiple virtual trees within DFS. DFS Namespaces was once known as Distributed File System in Windows 2000 Server and Windows Server 2003 (in case you still use Server 2003).

Now that you understand DFS and how it works, let's talk about DFS and Windows 10. Windows 10 allows you to use DFS by using the DFS client. After DFS is installed properly on the Windows Server 2012 R2 system, Windows 10 can then access the DFS namespace.

> **NOTE** Most Windows clients need to install the proper system updates to get the DFS drivers for client-side configurations. When deploying DFS, make sure your clients have all of their current updates.

DFS is a nice advantage for allowing users to find data, but now we are going to take a look at how your users can protect their data with data encryption. In the following section, we will discuss the benefits of using data encryption.

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 to users other than the person who encrypted the data. Once data has been encrypted, you must have the correct key to decrypt the data. Unencrypted data is known as plain text, and encrypted data is known as *ciphertext*.

The *Encrypting File System* (EFS) is the Windows 10 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. The following EFS features are among those included with Windows 10:

- Automatic color-coding of 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

In the following sections, you will learn how to encrypt and decrypt data, create and manage DRAs, recover encrypted files, share encrypted files, and use the Cipher utility.

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 it—even if those users have Full Control NTFS permissions. Instead, they will receive an error message.

> **NOTE** Windows 10 does not allow you to have a folder or file compressed and encrypted at the same time.

In Exercise 3.12, you will use EFS to encrypt a folder. Before encrypting any data, you will create a new user.

EXERCISE 3.12

Encrypting a Folder

1. To create a new user, right-click Start ➢ Computer Management. Under System Tools, expand Local Users And Groups and right-click the `Users` folder. Choose New User.

2. Create a new user named **Paige** and make her password **P@ssw0rd**. Deselect the User Must Change Password At Next Logon option for this user. Click Create.

3. Close Computer Management.

4. Select the File Explorer icon on the Taskbar.

5. In Windows Explorer, find and select a folder on the C: drive. The folder you select should contain files. Right-click the folder and select Properties.

6. On the General tab of the folder's Properties dialog box, click the Advanced button.

7. In the Advanced Attributes dialog box, check the Encrypt Contents To Secure Data option. Then click OK.

8. 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.

9. Log off as Administrator and log on as Paige.

10. 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.

11. Log off as Paige and log on as Administrator.

To decrypt folders and files, repeat the steps in Exercise 3.10, but uncheck the Encrypt Contents To Secure Data option in the Advanced Attributes dialog box.

The problem here is that the user who encrypts the data is the only one who can open the files. But the owner of the data can share the encrypted files with other users. In the next section, we will look at how to share your encrypted data with other users.

Managing EFS File Sharing

In Windows 10, it is possible to share encrypted files with other people or between multiple 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.

Complete Exercise 3.13 to implement EFS file sharing.

EXERCISE 3.13

Implementing EFS File Sharing

1. Encrypt the file if it is not already encrypted (see Exercise 3.12 for the steps involved).

2. Through Windows Explorer, access the encrypted file's properties. At the bottom of the dialog box, click the Advanced button.

3. The Advanced Attributes dialog box appears. 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.

4. In the Encryption Details dialog box, click the Add button to add any additional users who should have access to the encrypted file (provided they have a valid certificate for EFS in Active Directory or that you have imported a valid certificate onto the local computer).

5. Close the Properties box for the folder.

Recovering Encrypted Files

Someone may have encrypted files or folders and then left the company. There are a few different ways to unencrypt the data so you can continue to use the files or folders, as you'll see in the next sections.

Using the DRA

If a user who encrypted folders or files is unavailable or no longer with the company and you need to decrypt the folders or files, you can use the 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 10 computers that are a part of a Windows 2012 R2 Active Directory domain, the domain Administrator user account is automatically assigned the role of DRA.
- For Windows 10 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 10 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 10 Computer

If Windows 10 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 may use the Cipher command-line utility as follows:

```
Cipher/R:filename
```

The /R switch is used to generate two files, one with a .pfx filename 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. Cipher is explained further in the next section.

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 steps in Exercise 3.14.

E X E R C I S E   3 . 1 4

Using the Local Security Policy

1. Through Local Security Policy, which can be accessed through Administrative Tools or the Local Computer Policy MMC snap-in, expand Public Key Policies ➢ Encrypting File System (as shown in Figure 3.31).

FIGURE 3.31   Local Security Policy
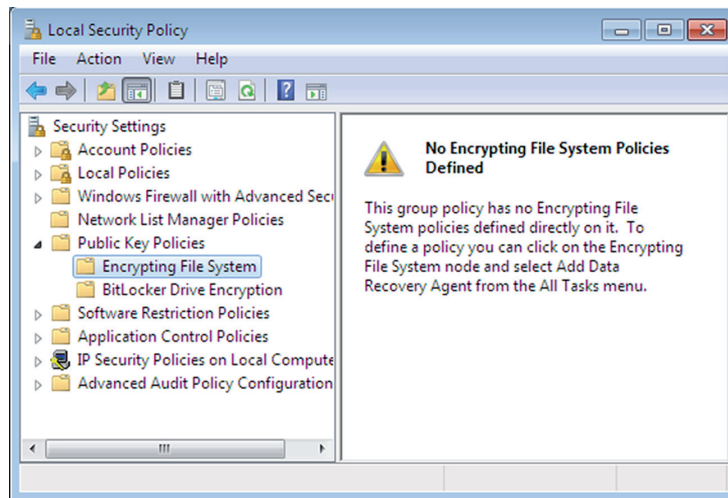
2.   Right-click Encrypting File System and select Add Data Recovery Agent.

3.   The Add Recovery Agent Wizard starts. Click the Next button to continue.

4.   The Select Recovery Agents screen appears (shown in Figure 3.32). Click the Browse Folders button to access the CER file you created with the `Cipher /R:`*`filename`* command. Select the certificate and click Next.

FIGURE 3.32   Select Recovery Agents
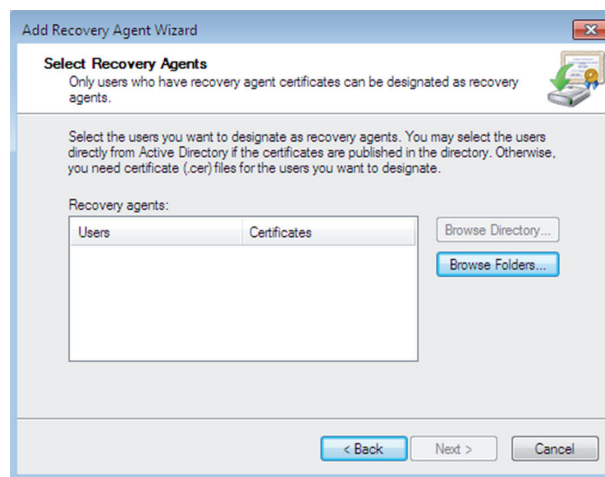
5.   The Completing The Add Recovery Agent Wizard screen appears. Confirm that the settings are correct and click the Finish button.

You will see the DRA listed in the Local Security Settings dialog box, under Encrypting File System. 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 3.6 lists common command parameters associated with the `Cipher` command.

TABLE 3.6   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 key into the specified filename.

Exercise 3.15 will show you how to use the Cipher utility to encrypt files. Make sure that you have encrypted a folder on the C: drive before completing these steps.

EXERCISE 3.15

Using the Cipher Utility

1. Right-click Start ➢ Command Prompt (Admin).

2. In the Command Prompt dialog box, type `C:` and press Enter to access the C: drive.

3. From the `C:\>` prompt, type `cipher`. You will see a list of folders and files and the state of encryption. The folder you encrypted should be indicated by an E.

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.

In the next section, we will look at how to protect your data using Redundant Array of Independent Disks.

Understanding RAID

One concern for any computer department is the loss of data due to hard-drive failures. *Redundant Array of Independent Disks (RAID)* allows an administrator to recover data from a single hard-disk failure.

The important factor to remember about Microsoft software-based RAID is that you can recover from only a single disk failure. If multiple hard disks fail, RAID will no longer protect your system from data loss.

There are two types of RAID (called *RAID models*): hardware based and software based. Hardware RAID, which is the best option, is built into the physical hardware and must be supported by the disk controllers and hard drives. Software RAID is configured through the Windows operating system.

The downside to hardware RAID is cost. A server or computer that has hardware RAID built in can cost thousands of dollars. Software RAID is free, but remember the old saying "You get what you pay for."

In the next section, we will look at the different models of RAID and how each model operates.

RAID Levels

There are many different levels of RAID, but Microsoft Windows 10 allows for configuration of three main levels: RAID-0, RAID-1, and RAID-5. Let's take a look at each:

RAID-0 (Striped)   RAID-0 has no data recoverability, but it is used for better performance. With RAID-0 you can have a minimum of two hard disks, and these two disks work together as a single volume. Because the two disks work together, the disks both use their own read/write heads, giving you better performance.

The downside to RAID-0 is that if you lose either disk, you lose the entire striped volume. RAID-0 is good for temp files or noncritical data since RAID-0 is not recoverable in the event of a single hard-disk failure.

RAID-1 (Mirroring)   RAID-1, also known as mirroring, allows you to set up two volumes or disks that mirror each other. The advantage to mirroring is that if you lose one disk or volume, you can boot to the second disk or volume (the mirror) and recover your data. The downside to mirroring is that it is more expensive than other RAID options.

RAID-5 Volume   A RAID-5 volume, which many years ago was known as a stripe set with parity, uses a minimum of 3 disks (maximum of 32 disks) that work together as one volume. The advantage to a RAID-5 volume is that the volume uses a parity bit, which allows you to recover your data in the event of a single hard-disk failure.

When it comes to hardware RAID and software RAID, recoverability is night and day. Hardware RAID is much faster and easier when a hard disk fails. Many hardware RAID systems are hot swappable, meaning that when a disk fails, you just slide it out, insert a new disk, and RAID gets back to work.

This is not the case with software RAID. Recovering from a single hard-disk failure can take time, which in turn costs an organization money. Software RAID is set up through the Disk Management utility (explained earlier in this chapter) and is not available unless you have multiple hard disks installed in the Windows 10 machine.

Storage Spaces

Storage Spaces in Windows 10 is another way to give your Windows 10 users data redundancy. This is just another advantage of Windows 10 and that advantage is called Storage Spaces. Windows 10 administrators have the ability to group hard drives together into a storage pool. Windows 10 users can then use these storage pool capacities to turn the pools into individual storage spaces.

Storage spaces then show up in File Explorer as regular drives, but they are actually virtual drives created using the storage spaces. Users can use these drives just like any other hard drive in their system.

But when you set up the Storage Spaces, you can set them up so if you have at least two drives in the storage pool, you can create storage spaces that won't be affected by a drive failure. This gives you fault tolerance on the user's data.

Now why is this an actual advantage for Windows 10? Well, one of the biggest issues we have as administrators is our users running out of hard drive space. If we decide to use Storage Spaces and the user starts to run out of space, administrators can add more drives and increase the storage space on the user's Windows 10 system while also getting fault tolerance on the data.

To create storage spaces, you need at least one or more hard drives besides the drive on which Windows 10 is installed. One huge advantage is that these hard drives can be either internal or external hard drives, including solid-state drives. When it comes to building storage spaces, there are three main unique kinds based on your storage needs. Each one works like a version of RAID:

Simple Spaces   Simple storage spaces work the same as RAID-0 (striped volumes). Simple spaces are designed to give users increased performance but no data protection. These spaces are used best for files that don't need to be protected (temp files, music, etc.). The works great when you want better performance, and simple spaces only require at least one drive.

Mirror Spaces   Mirror storage spaces work just like RAID-1 (mirror), and they are designed to give you better performance while also giving your data protection from a single hard drive failure for a two-way mirror and a double hard drive failure from a three-way mirror.

Administrators can take mirror storage spaces even further by formatting them with the Resilient File System (ReFS). If the mirror storage space is formatted using ReFS, Windows will then automatically maintain the mirror's data integrity, making your data even further resilient to hard drive failures.

Parity Spaces   Parity storage spaces work a lot like RAID 5 volumes (stripe set with parity). To use parity spaces you are required to have at least three drives to protect you from a single hard drive failure or seven drives to protect you from a double hard drive failure.

If you want to set up storage spaces, right-click the Start button and choose Control Panel. In the upper-right corner, change the View By option from Category to Large Icons. Scroll down to Storage Spaces and double-click Storage Spaces (see Figure 3.33).

FIGURE 3.33   The Storage Spaces icon in Control Panel
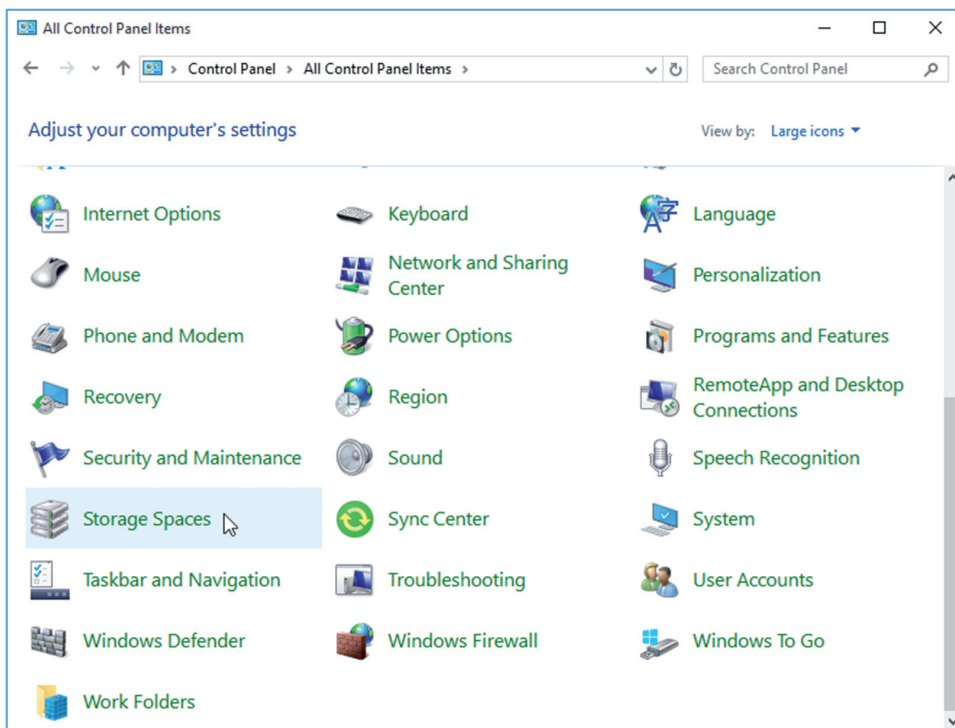
After you double-click and open Storage Spaces, you would complete the following steps to create a storage pool:

1. Click the "Create a new pool and storage space" link (shown in Figure 3.34).

FIGURE 3.34   The link to create a new pool and storage space
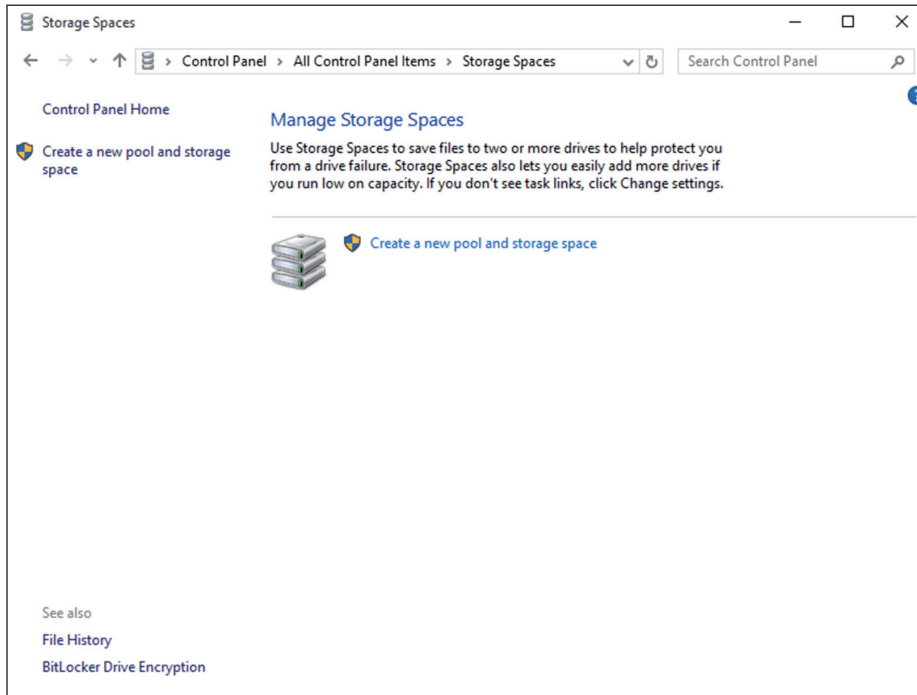
2. Select the drives you want to add to the new storage space, and then click or click Create Pool.

3. Give the drive a name and letter, and then choose a layout (Simple, Two-Way Mirror, Three-Way Mirror, or Parity).

4. Enter the maximum size the storage space can reach, and then click Create Storage Space.

Now that you have seen how you can protect your data, in the next section, we will look at how you can keep your disk volumes and partitions running at peak performance.

Using Disk-Maintenance Tools

Part of our job as IT professionals is to keep our systems running the best that they can. Most of us have seen machines running very quickly when they are new, but then they start to slow down over time, even when we do not install any new software.

Microsoft Windows 10 includes a few utilities that you can run to help keep your system running efficiently. In the next sections we will discuss three of these utilities: Disk Optimization utility, Disk Cleanup, and Check Disk.

Using the Disk Optimization Utility

Data is normally stored sequentially on the disk as space is available. Optimization 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 optimization rearranges the existing files so they are stored contiguously, which optimizes access to them. In Windows 10, you use the Disk Optimization utility to optimize and defragment your disk.

To access the Disk Optimization utility, right-click Start ➢ Computer Management. Expand Storage and select Disk Management, right-click the drive, select the Tools tab, and then click the Optimize button. The Optimize window appears (Figure 3.35); you can schedule when the disk optimizer should run or run the tool immediately.

FIGURE 3.35   The Optimize Drives window
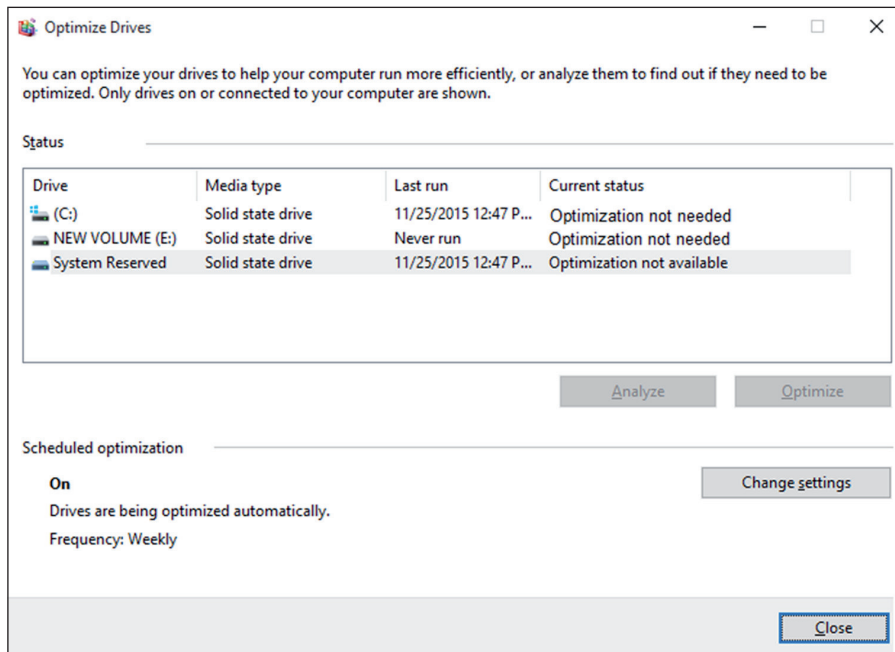
In the next section we will look at another tool that is included with Windows 10—the Disk Cleanup utility.

Using the Disk Cleanup Utility

One concern that we as IT professionals face is how to conserve hard-disk space for our users. Hard drives continue to get larger and larger, but so do applications. This is where the Disk Cleanup utility can help.

The Disk Cleanup utility identifies areas of disk space that can be deleted to free up hard-disk space. Disk Cleanup works by identifying temporary files, Internet cache files, and unnecessary program files.

To access this utility, right-click Start ➢ Computer Management. Right-click the drive letter and choose Properties and then Disk Cleanup. The Disk Cleanup utility then runs and calculates the amount of disk space you can free up.

Complete Exercise 3.16 to run the Disk Cleanup utility on the Windows 10 operating system.

EXERCISE 3.16

Running the Disk Cleanup Utility

1. Right-click Start ➢ Computer Management.

2. Right-click the drive and choose Properties.

3. On the General tab, click the Disk Cleanup button.

   The Disk Cleanup utility will start to calculate the system data.

4. After the analysis is complete, you will see the Disk Cleanup dialog box (shown in Figure 3.36) listing files that are suggested for deletion and showing how much space will be gained by deleting those files. Click OK.

FIGURE 3.36 The Disk Cleanup dialog box
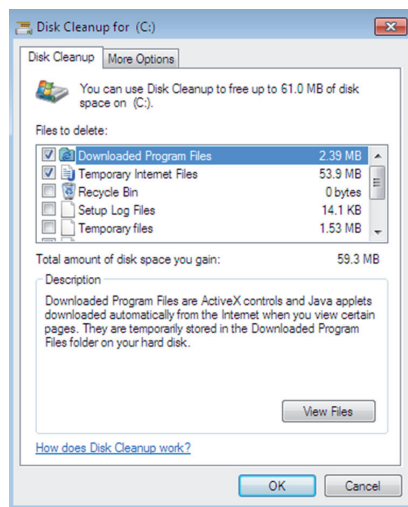
5. When you are asked to confirm that you want to delete the files, click the Yes button. The Disk Cleanup utility deletes the files and automatically closes the Disk Cleanup dialog box.

Another issue that you may run into is bad sectors on your hard disk. Windows 10 also includes a utility to help you troubleshoot disk devices and volumes.

Using the Check Disk Utility

If you are having trouble with your disk devices or volumes, you can use the Windows 10 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. 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.

Complete Exercise 3.17 to run the Check Disk utility.

EXERCISE 3.17

Using the Check Disk Utility

1. Select Start ➢ Computer Management, and then expand Storage and select Disk Management.

2. Right-click the C: drive and choose Properties.

3. Click the Tools tab, and then click the Check Now button.

4. In the Check Disk dialog box (shown in Figure 3.37), 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 check boxes. Then click the Start button.

FIGURE 3.37   The Check Disk dialog box
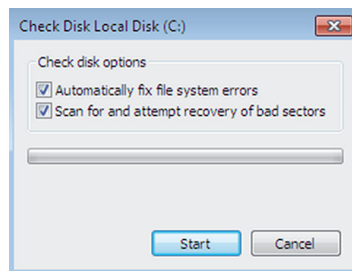
Another way to run the Check Disk utility is from the command line, using the command Chkdsk. Chkdsk is used to create and display a status report, which is based on the file system you are using.

Summary

There are two different ways that you can format your hard disk in a Windows 10 operating system: FAT32 and NTFS. NTFS has many advantages over FAT32, including security, encryption, disk quotas, and compression, just to name a few.

Besides the way you format your hard disk, you can configure your hard disk as a basic disk or a dynamic disk and must choose to either leave your disk partition system as the default MBR or choose to convert it to a GPT disk. You can use the Disk Management MMC snap-in to configure your hard disks and file system.

Another configurable option within the Disk Management utility is RAID. RAID-1 and RAID-5 allow you to recover your data in the event of a single hard-disk failure. RAID-0 allows you to achieve better performance but has no data recoverability in the event of a hard-disk failure. You also have Storage Spaces, which gives your data a way to have recoverability and larger disk pools.

After the hard disks are installed and configured, there will be some maintenance items that need to be tended to. The utilities that allow you to perform these maintenance activities include the Disk Defragmenter and Check Disk utilities.

In the next chapter, we will examine how to manage data access on the Windows 10 operating system.

Video Resources

There are videos available for the following exercises:

    3.1

    3.2

    3.4

You can access the videos at www.wiley.com/go/sybextestprep on the Other Study Tools tab.

Exam Essentials

Understand the different file format options.   There are two ways to format a hard disk in Windows 10: FAT32 and NTFS. Understand that NTFS offers many benefits over FAT32, including security, encryption, compression, and disk quotas.

Understand the different hard-disk storage types.   Windows 10 supports three types of disk storage: basic, dynamic, and GUID Partition Table (GPT). Basic storage is backward compatible with other operating systems and can be configured to support up to four partitions. Dynamic storage is supported by all Windows operating systems above Windows 2000 and allows storage to be configured as volumes. GPT storage allows you to configure volume sizes larger than 2 TB and up to 128 primary partitions.

Know Storage Spaces.   Microsoft Windows 10 includes Storage Spaces, which can help you create disks into storage pools, which can then be turned into storage spaces. Storage spaces allow you to take multiple disks and create drives with fault tolerance.

Understand Encrypted File Systems   Know that data encryption is a way to increase data security. Encryption is the process of translating data into code that is not easily accessible to users other than the person who encrypted the data.

Understand Distributed File Systems   Distributed File System (DFS) in Windows Server 2012 R2 offers a simplified way for users to access geographically dispersed files. DFS allows you to set up a tree structure of virtual directories that allow users to connect to shared folders throughout the entire network.

Know the disk-management utilities.   Microsoft Windows 10 includes a few utilities that you can run to help keep your system running efficiently. These utilities include Disk Defragmenter, Disk Cleanup, and Check Disk.

Review Questions

1. Will has installed Windows 10 on his Windows XP computer. The machine is now a dual-boot computer. He has FAT32 for Windows XP and NTFS for Windows 10. In addition, he boots his computer to Windows XP Professional for testing an application's 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. You are the network administrator for a large company that has decided to use EFS. You have two Windows 10 machines, named machine1 and machine2. Both of these Windows 10 machines are part of a Windows Server 2012 R2 domain. From machine1, you can recover all EFS encrypted files for all users in the entire domain. You need to be able to do the same from machine2. How do you accomplish this task?

   A. From machine1, export the DRA certificate and import that certificate onto machine2.

   B. On a domain controller, add machine1 as the master EFS machine.

   C. From machine1, export the DRA certificate and import that certificate onto the EFS server.

   D. On a domain controller, add machine2 as the EFS recovery agent machine.

3. Alexandria is the payroll manager and stores critical files on her local drive for added security on her Windows 10 computer. She wants to ensure that she is using the disk configuration with the most fault tolerance and the highest level of consistent availability. Which of the following provisions should she use?

   A. Disk striping

   B. Spanned volumes

   C. Mirrored volumes

   D. Extended volumes

4. Paige is considering upgrading her basic disk to a dynamic disk on her Windows 10 computer. She asks you to help her understand the function of dynamic disks. Which of the following statements are true of dynamic disks in Windows 10?

   A. Dynamic disks can be recognized by older operating systems such as Windows NT 4 in addition to new operating systems such as Windows 10.

   B. Dynamic disks are supported only by Windows 2000 Server and Windows Server 2003.

   C. Dynamic disks support features such as simple partitions, extended partitions, spanned partitions, and striped partitions.

    D. Dynamic disks support features such as simple volumes, extended volumes, spanned volumes, mirrored volumes, and striped volumes.

5. Cindy is using Windows 10 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. Rob is using Windows 10 to store video files. He doesn't access the files very often and wants to compress the files to utilize disk space more effectively. Which of the following options allows you to compress files in Windows 10?

    A. `JetPack.exe`

    B. `Cipher.exe`

    C. `Packer.exe`

    D. Windows Explorer

7. Crystal 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. EDS

8. You have compressed a 4 MB file into 2 MB. 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, Tylor, access to several files that she has encrypted with EFS. How can she allow Tylor to access the files on her computer?

    A. Julie should export and email her encryption key to Tylor.

    B. Julie should configure NTFS permissions to provide Tylor with full access to the files.

    C. Julie should import Tylor's encryption key and add Tylor's certificate to each file to which Tylor should have access.

    D. Julie should configure share permissions to provide Tylor with full access to the files over the network.

10. Will 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. How can you apply the highest level of security 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.

Chapter

4

Managing Data Access

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Support data security.**

- This objective may include but is not limited to the following subobjectives: Identifying and resolving issues related to the following: Permissions including share, NTFS, and Dynamic Access Control (DAC); access to removable media; BitLocker and BitLocker To Go including Data Recovery Agent and Microsoft BitLocker Administration and Monitoring (MBAM).

✓ **Configure shared resources.**

- This objective may include but is not limited to the following subobjectives: Configure shared folder permissions, configure HomeGroup settings, configure libraries, configure shared printers, configure OneDrive.

✓ **Configure security for mobile devices.**

- This objective may include but is not limited to the following subobjectives: Configure BitLocker, configure startup key storage.

One of the most fundamental tasks in network management is setting up user's rights and permissions. This is by far one of the most important tasks that we as IT members face every day. Too much access and your users can cause issue. Not enough access and your users can't do their job.

One way to help make sure that your users don't have more permissions or security than they need is to use groups. Groups are used to ease network administration by grouping users together who have similar permission requirements. Groups are an important part of network management.

We will dive into user accounts and groups in Chapter 8, "Managing Identity and Authorization," but you still need to understand how NTFS and shared resources work together and how to secure the network hardware. So that's where this chapter comes into play.

In this chapter, we will also talk about users accessing resources on a network. If you think about it, that's one of the main reasons we set up networks, to share resources. If we didn't have resources that users needed access to, why even bother setting up a network? So we will talk about sharing resources and assigning permissions to those shares.

You will then learn about NTFS security and share permissions and how they work independently and together. Finally, this chapter will introduce you to some of the Windows 10 security options, including BitLocker. So let's start exploring ways to make your data more secure.

Managing File and Folder Security

Setting up proper file and folder security is one of the most important tasks that an IT professional can perform. If permissions and security are not properly configured, users will be able to access resources that they shouldn't. 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 10, 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.

When a user is created on a local Windows 10 system or if the user is created on an Active Directory domain, the user gets a Security Identification (SID) number. It is important to remember that when you assign rights to a user, those rights and permissions get

associated to the user's SID number and not the username. It's because of this that we can rename user accounts without any issues.

Before diving into the security nitty-gritty, you need to know about the folder options. So let's start with that discussion.

Folder Options

The Windows 10 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, right-click Start ➤ File Explorer and then select View and then Option. You can also access Folder Options by choosing Control Panel ➤ *Large Icons View* ➤ File Explorer 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, shown in Figure 4.1, includes the following options:

- 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
- Whether to have the navigation pane show all folders and automatically expand to the current folder

FIGURE 4.1   The General tab of the Folder Options dialog box
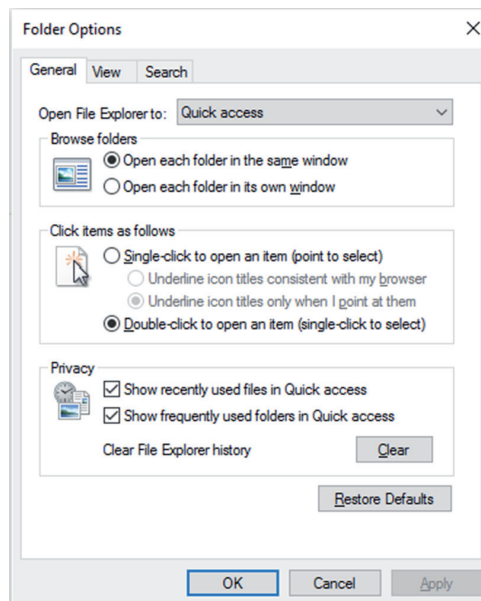
Folder View Options

The View tab of the Folder Options dialog box, shown in Figure 4.2, is 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 4.1 describes the View tab options.

FIGURE 4.2   The View tab of the Folder Options dialog box
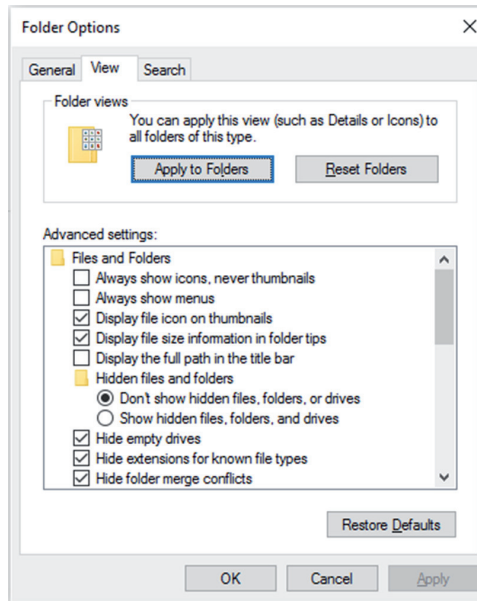
TABLE 4.1   Folder view options

Option	Description	Default
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 you're browsing for files.	Not selected
Display File Icon On Thumbnails	Displays the file icon on thumbnails.	Selected

Option	Description	Default
Display File Size Information In Folder Tips	Specifies whether the file size is automatically displayed when you hover your mouse over a folder.	Selected
Display The Full Path In The Title Bar (Classic Theme Only)	Specifies whether the title bar shows an abbreviated path of your location. Selecting this option displays the full path, such as `C:\Word Documents\ Sybex\Windows 10 Book\Chapter 9`, as opposed to showing an abbreviated path, such as `Chapter 9`.	Not selected
Hidden Files And Folders	Specifies whether files and folders with the Hidden attribute are listed. Choosing Show Hidden Files, Folders, Or Drives displays these items.	Don't Show Hidden Files, Folders, And Drives
Hide Empty Drives	Prevents drives that are empty in the `Computer` folder from being displayed.	Selected
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.	Selected
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. Deselecting this option displays the operating system files.	Selected
Launch Folder Windows In A Separate Process	By default, when you open a folder, it shares memory with the previous folders that were opened. Selecting this option opens folders in separate parts of memory, which increases the stability of Windows 10 but can slightly decrease the performance of the computer.	Not selected
Show Drive Letters	Specifies whether drive letters are shown in the `Computer` folder. When this option is disabled, only the name of the disk or device will be shown.	Selected

TABLE 4.1   Folder view options *(continued)*

Option	Description	Default
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.	Selected
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.	Selected
Show Preview Handlers In Preview Pane	Shows the contents of files in the preview pane.	Selected
Use Check Boxes To Select Items	Adds a check box next 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)	Allows you to share a folder using a simplified sharing method.	Selected
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 Options

The Search tab of the Folder Options dialog box, shown in Figure 4.3, is used to configure how Windows 10 searches for files. You can choose for Windows 10 to search by filename only, by filenames and contents, or by 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 in file folders for system files
- Include system directories in non-indexed locations
- Include compressed files in non-indexed locations

FIGURE 4.3   The Search tab of the Folder Options dialog box
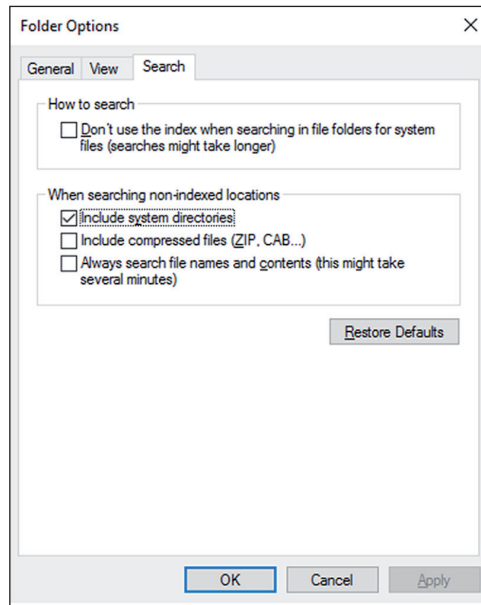
To search for files and folders, click Start ➢ Search and type your query in the search box.

Understanding Dynamic Access Control

One of the advantages of Windows Server 2012 R2 and Windows 10 is the ability to apply data governance to your file server. This will help control who has access to information and auditing. You get these advantages through the use of Dynamic Access Control (DAC). DAC allows you to identify data by using data classifications (both automatic and manual) and then control access to these files based on these classifications.

DAC also gives administrators the ability to control file access by using a central access policy. This central access policy will also allow an administrator to set up audit access to files for reporting and forensic investigation.

DAC allows an administrator to set up Active Directory Rights Management Service (AD RMS) encryption for Microsoft Office documents. For example, you can set up encryption for any documents that contain financial information.

DAC gives an administrator the flexibility to configure file access and auditing to domain-based file servers. To do this, DAC controls claims in the authentication token, resource properties, and conditional expressions within permission and auditing entries.

Administrators have the ability to give users access to files and folders based on Active Directory attributes. For example, a user named Dana is given access to the file server share because in the user's Active Directory (department attribute) properties, the value contains the value Sales.

Securing Access to Files and Folders

On NTFS partitions, you can specify the access each user has to specific folders or files on the partition based on the user's logon name and group associations. Access control consists of rights (which pertain to operations on the system) and permissions (which pertain to 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; explicit denials override 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.

Considering 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. The following list includes some of the considerations for planning access control:

▪   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, including defining the resources and defining the risk of damage if the resource is 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 10 clients are part of an Active Directory network

▪   Using additional security features, such as Encrypted File System (EFS), to provide additional levels of security or file auditing to track access to critical files and folders

   After you have decided what your design goals are, you can start applying your NTFS permissions.

Applying NTFS Permissions

NTFS permissions control access to NTFS files and folders. Ultimately, the person who owns an object has complete control over the object. The owner or administrator can configure access by allowing or denying NTFS permissions to users and groups.

   Normally, NTFS permissions are cumulative, based on group memberships. The user gets the highest level of security from all the different groups they belong to. However, if the user had been denied access through user or group membership, those deny permissions override the allowed permissions. Windows 10 offers seven levels of NTFS permissions, plus special 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.

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 section "Creating and Managing Shared Folders," later in this chapter.

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.

Special Permissions   This allows you to configure any permissions beyond the normal permissions, such as auditing, and to take ownership. To apply NTFS permissions, right-click the file or folder to which you want to control access, select Properties from the context menu, and then select the Security tab. The Security tab lists the users and groups who 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 (see Figure 4.4).

F I G U R E 4 . 4   The object's Security tab
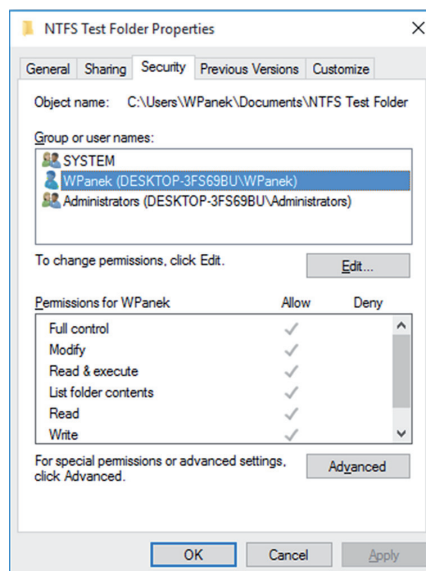
Exercise 4.1 walks you through assigning NTFS permissions.

Managing NTFS Permissions

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. 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.

    Through the Advanced button of the Security tab, you can configure more granular NTFS permissions, such as Traverse Folder and Read Attributes permissions.

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. 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 10.

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 10, 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*.

You can specify how permissions are inherited by subfolders and files by clicking the Advanced button on the Security tab of a folder's Properties dialog box. This calls up the Permissions tab of the Advanced Security Settings dialog box. To edit these options, click the Change Permissions button. You can edit the following options:

- Include Inheritable Permissions From This Object's Parent
- Replace All Existing Inheritable Permissions On All Descendants With Inheritable Permissions From This Object

If an Allow or Deny item 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 a 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 who owns the object
- The users and groups who 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 by clicking the Advanced button. Then click the Owner tab to see who the owner of the object is. From this dialog box, you can change the owner of the object.

Although the owner of an object can set its permissions so that the administrator can't access it, 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 subobjects of the object. If you would like to see who owns a directory, from the command prompt, type `dir /q`.

Determining and Viewing Effective Permissions for NTFS

To determine a user's effective permissions (the aggregate permissions the user 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 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, so she effectively has Modify (the highest right).

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	
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.

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.

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 permissions. 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.

One issue that IT people run into is what happens to the security when you move or copy a file or folder. Let's take a look at NTFS permissions when they are moved or copied.

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. Use the following guidelines 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.

User's permissions and rights are automatically assigned to the user's Security ID (SID) number and not the username. Because of this, you can rename user accounts. By renaming an account, you can give someone all the rights and permissions that someone else had who left the company. This is also why you can change someone's name if needed without changing their rights.

Managing Network Access

In every network, there are resources to which the users need to gain access. As IT professionals, we share these resources so that our users can do their jobs.

Sharing is the process of allowing network users access to a resource located on a 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 and configure share permissions.

Creating and Managing 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, where you can add local users. Alternatively, you can access the wizard by right-clicking a folder and then selecting Properties ➢ Sharing tab ➢ Share button.

However, you cannot use the Sharing Wizard to share resources with domain users. To share a folder with domain users, right-click the folder and select Properties, and then select the Sharing tab, shown in Figure 4.5.

FIGURE 4.5 The Sharing tab of a folder's Properties dialog box
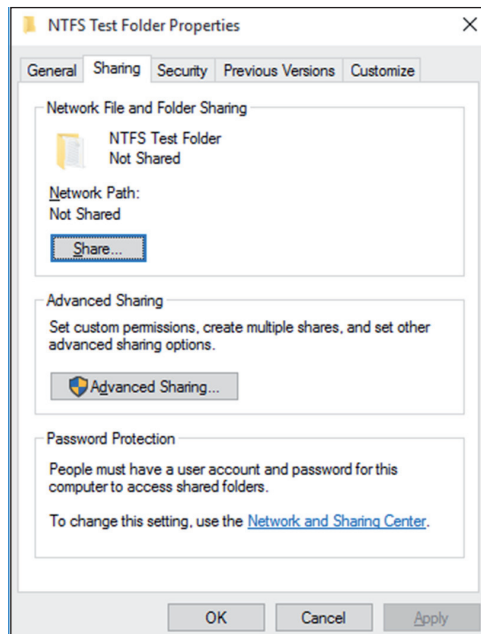
The Share button will take you to the Sharing Wizard. To configure Advanced Sharing, click the Advanced Sharing button, which will open the Advanced Sharing dialog box.

When you share a folder, you can configure the options listed in Table 4.2.

TABLE 4.2 Shared 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 10 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.

Keep in mind the following guidelines regarding sharing:

- 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.

Now let's take a look at configuring share permissions for your users.

Configuring Share Permissions

You can control users' access to shared folders from the network 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 Share Permissions dialog box, shown in Figure 4.6.

FIGURE 4.6   The Share Permissions dialog box
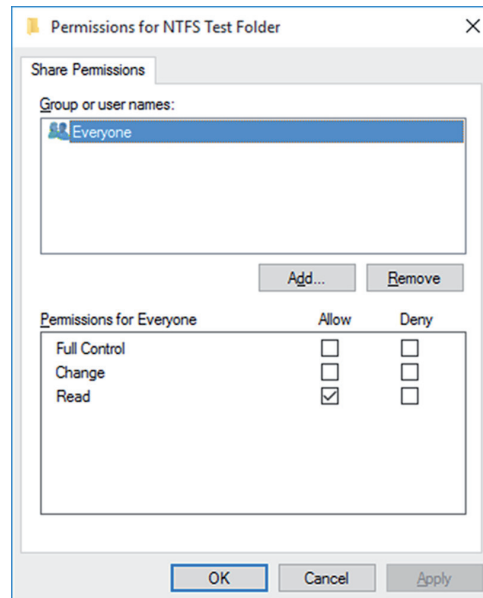
You can assign three types of share permissions:

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. Read 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. One thing that is the same between shared and NTFS is that all shared permissions are additive if you belong to multiple groups. This means that you add up all the permissions of the groups and get the highest permission.

When applying conflicting share and NTFS permissions, the most restrictive permissions win. 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. So, for example, if a user's NTFS security setting on a resource is

Read and the share permission on the same resource is Full Control, the user would have only Read permission when they connect to the shared resource. The most restrictive set of permissions wins.

Configuring OneDrive

Windows 10 includes Microsoft OneDrive with the operating system. Microsoft OneDrive is a cloud-based storage system where corporate users or home users can store their data in the cloud. Microsoft OneDrive allows users to use up to 15 GB of cloud storage for free without a subscription. Users have the ability to get more cloud-based storage by purchasing a higher subscription.

To set up a corporate user or home user with Microsoft OneDrive, you must first have a Microsoft account. You can create a Microsoft account at the time you are accessing OneDrive, as shown in Figure 4.7.

FIGURE 4.7 Microsoft OneDrive sign-in screen
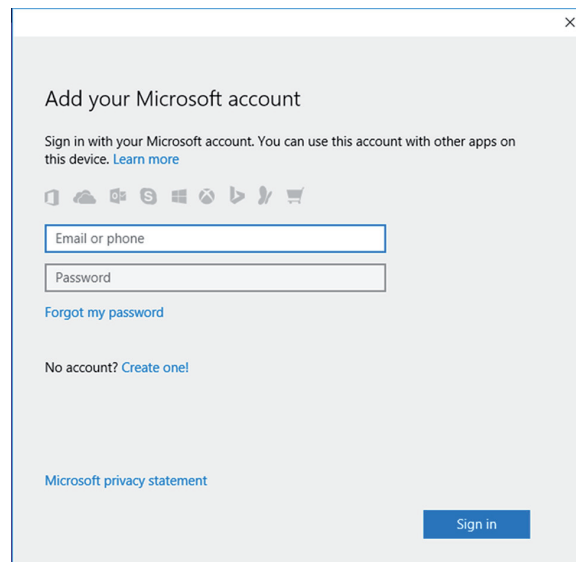
Once you have a Microsoft account, you then sign into the Microsoft OneDrive system where you can begin uploading data. Figure 4.8 shows Microsoft OneDrive from the Internet browser. Using the Internet browser, you can control the files that are located in the cloud.

FIGURE 4.8 Microsoft OneDrive
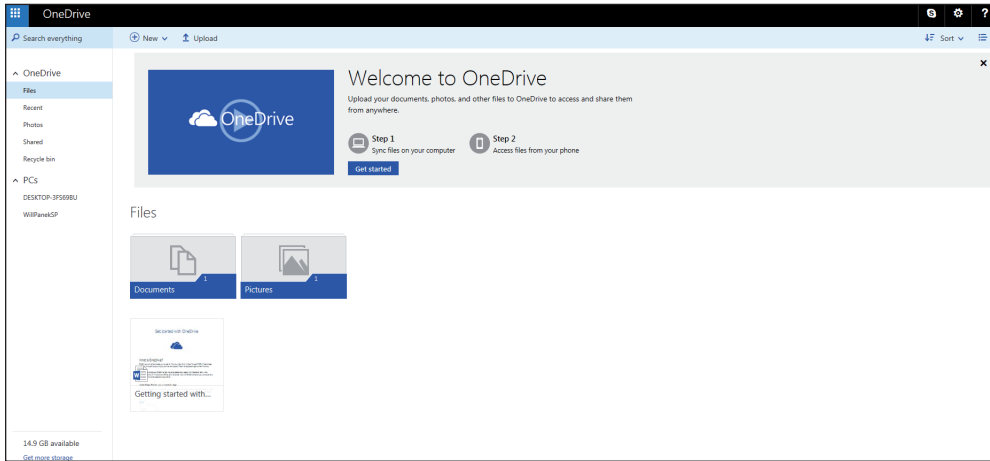
In Exercise 4.2, I will show you how to sign into your Microsoft OneDrive application.

Logging into OneDrive

1. Click the Start button ➢ All Apps ➢ OneDrive, as shown in Figure 4.9.

   FIGURE 4.9 OneDrive menu option
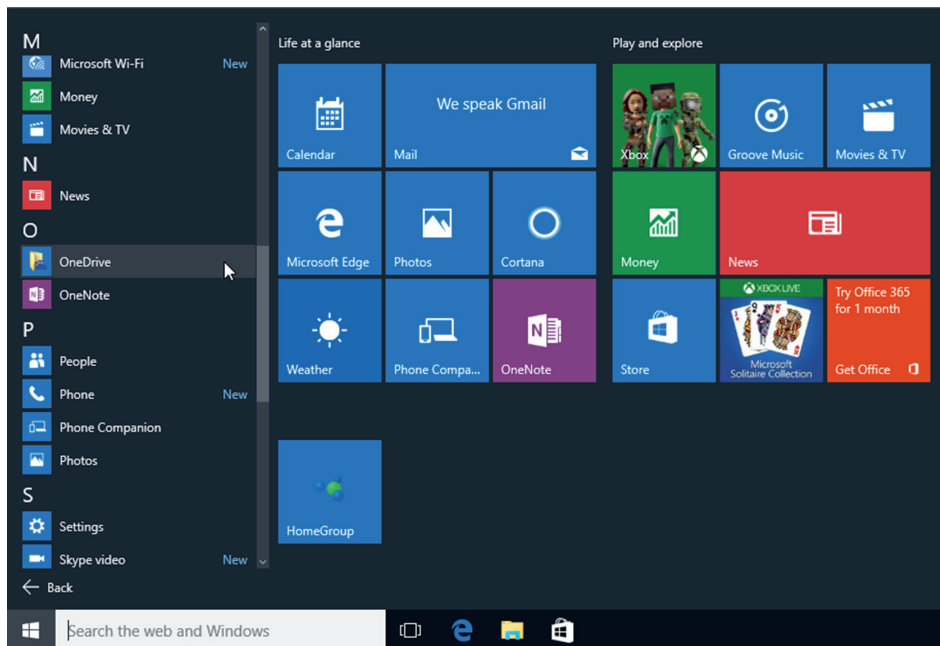
2. A screen will appear asking you to log on with Personal Microsoft account. Click the Sign In button.

3. On the Add Your Microsoft Account screen, type in your Microsoft account name and password to log in, as shown in Figure 4.10.

   FIGURE 4.10   OneDrive login
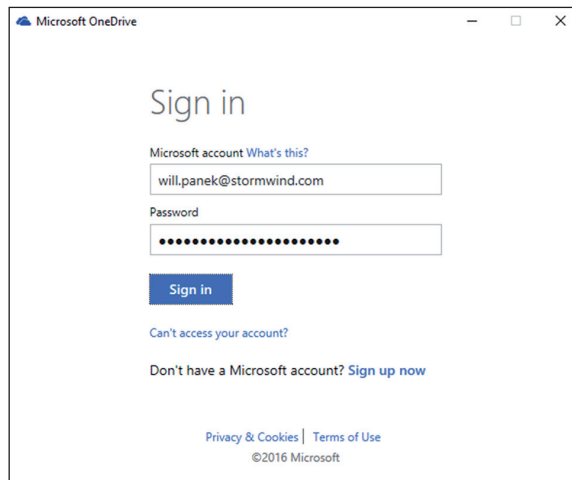
4. Another screen will appear stating that this is your OneDrive folder (shown in Figure 4.11). Click Next.

   FIGURE 4.11   This is your OneDrive folder screen.
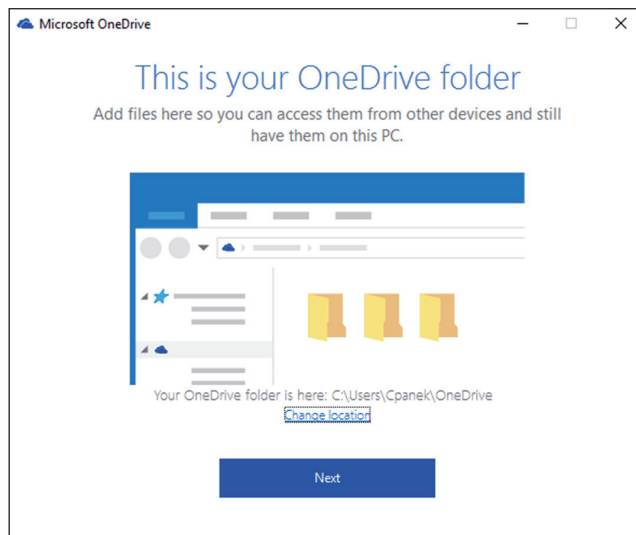
5. The next screen will allow you to sync files with OneDrive. Choose which folders you want to sync and click Next, as shown in Figure 4.12.

FIGURE 4.12   Sync files screen
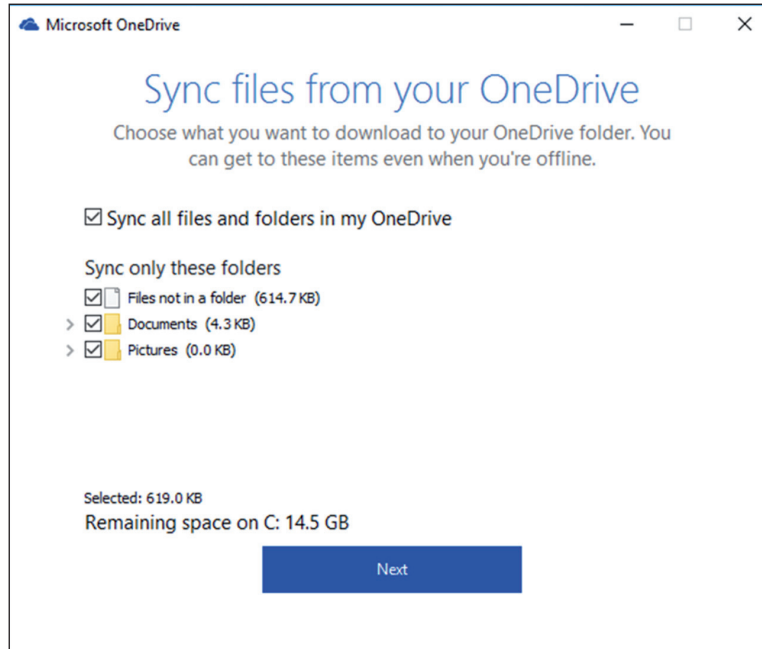
6. The next screen will tell you that you can start using OneDrive. Click the Open My OneDrive Folder button.

At this point you can start using OneDrive to create and upload files to the OneDrive cloud. In the left corner, next to the Home tab, you will see three lines. If you click those three lines, some options will appear. The bottom option allows you to change the OneDrive settings.

Inside those settings, you have the ability to change how often the system will sync with the cloud, which accounts will be associated to this OneDrive, and many other settings. The OneDrive cloud-based storage is a good way to back up some documents for protection of data loss.

When Windows 7 was released, Microsoft created an easy way for users to set up networks at home even if they don't know much about networking. In the next section, we will look at using Windows 10 HomeGroups.

Joining and Sharing HomeGroups in Windows 10

HomeGroup is a functionality of Windows 10 that simplifies the sharing of music, pictures, and documents within your small office or home network of Windows 10 PCs. HomeGroup allows you to share USB-connected printers too. If you have a printer installed on a Windows 10 computer and it's shared by HomeGroup, it is automatically installed onto the other HomeGroup-enabled Windows 10 PCs. Domain-joined computers cannot host a HomeGroup, but they can be a participant of a HomeGroup. All editions of Windows 10 can use HomeGroups, but only Home, Enterprise, or Professional edition can create a HomeGroup.

The first step in the process of using HomeGroup for sharing is to create a new HomeGroup or join an existing one. If the Windows 10 network-discovery feature does not find a HomeGroup, you will be asked to create a HomeGroup. In the Network and Sharing Center, select Choose HomeGroup and then click the Create A HomeGroup button (Figure 4.13).

FIGURE 4.13 Create a HomeGroup.
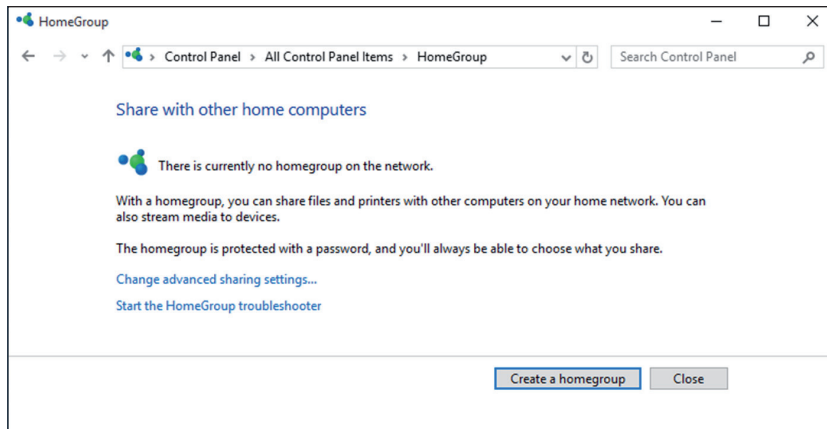
With Windows 10 network discovery turned on (the default), a HomeGroup is created automatically. You still need to join the HomeGroup to use the other shared resources and to share yours. From the Network and Sharing Center, you can join an existing HomeGroup by clicking the Join Now button, as shown in Figure 4.14.

Part of joining a HomeGroup setup is defining the libraries that you want to make available to the other members of the HomeGroup. The HomeGroup libraries are the folders (Pictures, Music, Videos, Documents, and Printers) that you want to share. So you can choose which HomeGroup libraries that you want to share or not share. The next screen in the setup (Figure 4.15) lets you choose which resources you want to share.

FIGURE 4.14   Join an existing HomeGroup.
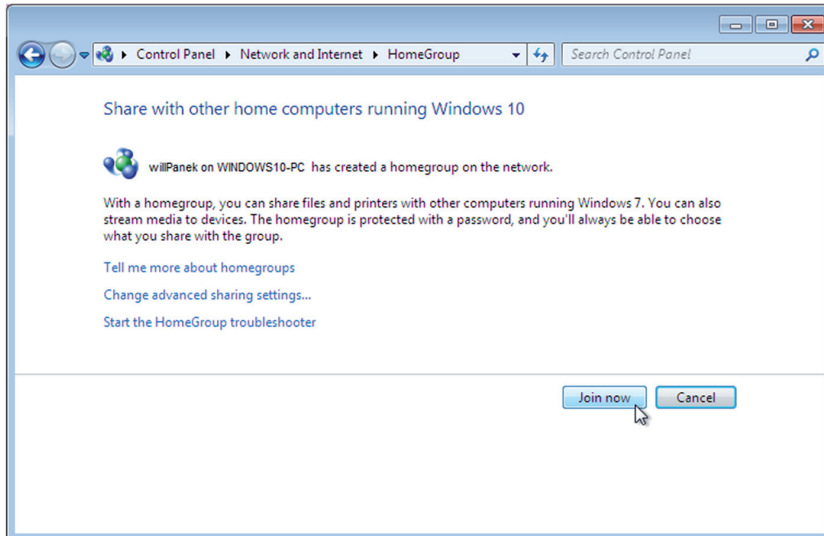
FIGURE 4.15   HomeGroup sharing selections
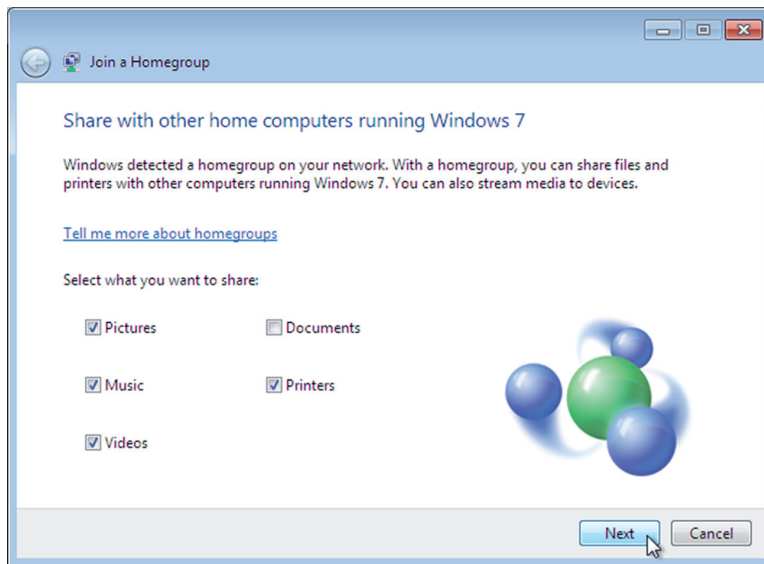
The next step is to enter the HomeGroup password. Windows 10, by default, will recognize a HomeGroup on the network. However, the other Windows 10 machines will not have access to the resources. Allowing any Windows 10 machine connecting to the network to automatically have shared resource access would be a huge security hole. To protect the Windows 10 user resources, a password must be entered to join a HomeGroup.

The password for the HomeGroup can be viewed or changed on the machine that established the HomeGroup. After other machines have joined, each machine has the ability to view or change the password. The initial machine in the HomeGroup will create a random secure password. To view and/or print the HomeGroup password, use the Choose HomeGroup And Sharing Options selection from the Network and Sharing Center, and then choose View Or Print The HomeGroup Password item, shown in Figure 4.16. Again, this can be done from any Windows 10 machine that is already a member of the HomeGroup but not from one that wants to join.

FIGURE 4.16   Change HomeGroup Settings screen
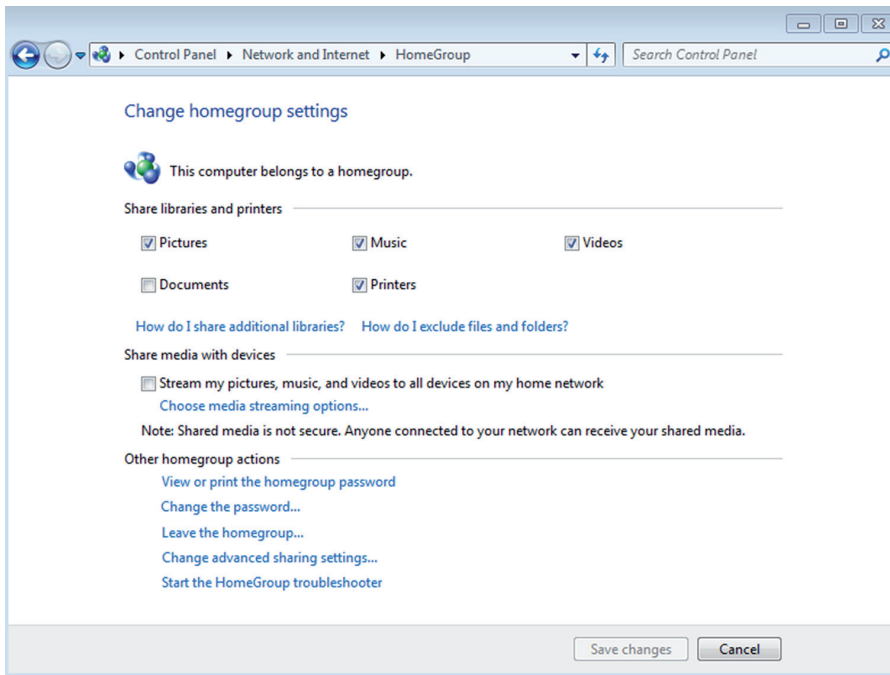
Figure 4.17 shows the View And Print Your HomeGroup Password screen. For simplicity here, I have changed the password to *password*, which is an example only and not recommended for your network.

FIGURE 4.17   View And Print Your HomeGroup Password screen
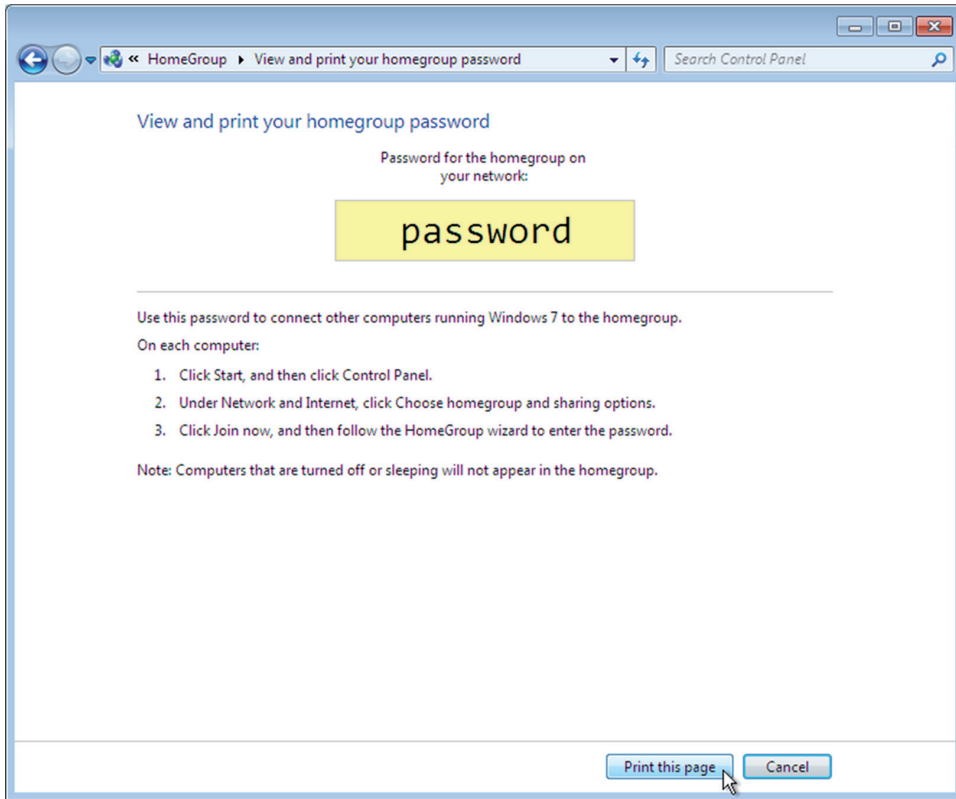
Remember that Windows 10 will initially create a random secure password for the HomeGroup, and you need to visit the View And Print Your HomeGroup Password screen to find out what it is. You will probably want to change it. To change the password, choose the Change The Password option from the Change HomeGroup Settings page and then select Change The Password from the Change Your HomeGroup Password screen, as shown in Figure 4.18. When you change the HomeGroup password, you need to go to each of the other Windows 10 machines that are members of the HomeGroup and change the password there if you still want the others to share resources.

After the HomeGroup is set up, you can see the other members' resources from the HomeGroup option of Windows Explorer or even the Start menu if you customize the Start menu and have added HomeGroup to the displayed options. I have added the HomeGroup

option to my Start menu, as shown in Figure 4.19. To add the HomeGroup to the Start menu, right-click the Start menu and choose Control Panel. Once in Control Panel, make sure the view is set to Large Icons (in the upper-right corner of the window). Right-click the HomeGroup icon and choose Pin To My Start.

FIGURE 4.18   Change the HomeGroup password.
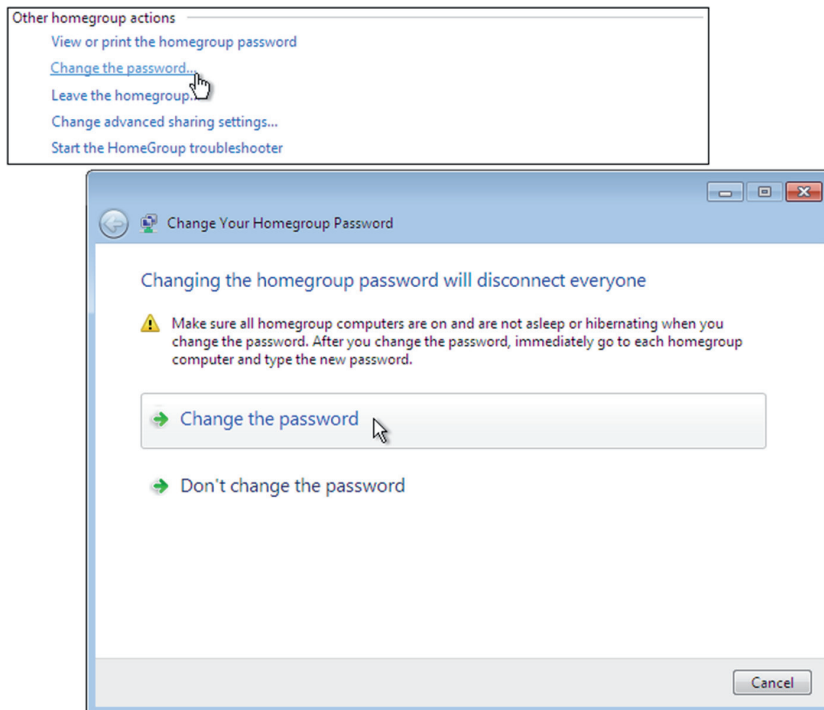
HomeGroups are a great option for users who want to share resources in the Windows 10 environment. But what if you still have non–Windows 10 machines? The legacy function of simply sharing resources and setting permissions still works for Windows 10 and will allow older operating systems to have access to resources shared on Windows 10 machines as well as allow users running Windows 10 to have access to the shared resources on older Windows operating systems.

In the following sections, I will show you how to start protecting your hardware from data loss or theft by securing your hardware.

FIGURE 4.19   HomeGroup in the Start menu
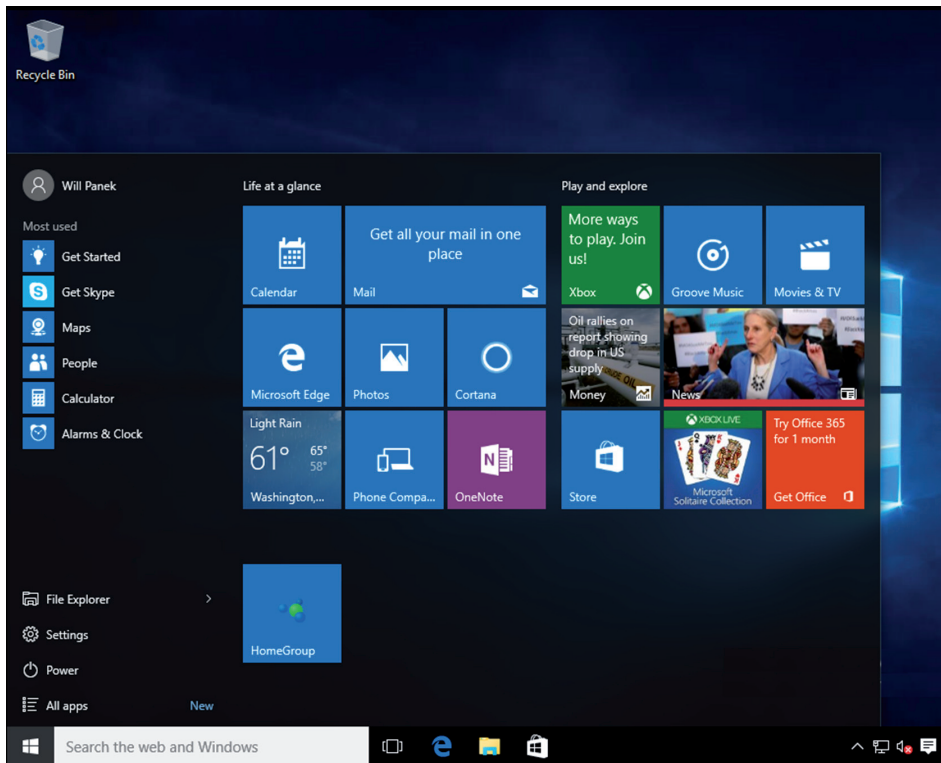
Understanding Hardware Security

One issue that IT members have to face is the protection of not only our data but also the hardware that the data resides on. (You may remember a case a few years back when an individual stole some hard drives from a VA office.) Let's take a look at a security measure that will help you protect your data drives from physically being taken.

We must make sure that if anyone steals hardware from our corporation or from our server rooms that the data that they are stealing is secured and can't be used. This is where BitLocker can help.

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 come with a new feature called *BitLocker Drive Encryption*. BitLocker encrypts the entire system drive.

BitLocker allows you to configure security for mobile devices by locking the physical drives. If someone steals a hard drive or external drive that has BitLocker on the drive, that drive will not function properly on another computer system.

When you use BitLocker, new files added to the BitLocker drive are encrypted automatically, and files moved from this drive to another drive or computers are decrypted automatically.

Only Windows 10 Enterprise, Professional, and Education, Windows 8 Pro and Enterprise, Windows 7 Pro and Enterprise, Windows Server 2008 and 2008 R2, and Windows Server 2012 and 2012 R2 include BitLocker Drive Encryption, and only the operating system drive (usually `C:`) or internal hard drives can be encrypted with BitLocker. Files on other types of drives must be encrypted using BitLocker To Go. BitLocker To Go allows you to put BitLocker on removable media such as external hard disks or USB drives.

BitLocker uses a Trusted Platform Module (TPM) version 1.2 or higher to store the security startup 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 startup key on a removable USB drive. If you don't have a system with TPM, you will need to turn off the TPM setting in the local computer settings as shown in Figure 4.20. The USB drive will be required each time you start the computer so that the system drive can be decrypted.

FIGURE 4.20 Changing the TPM settings
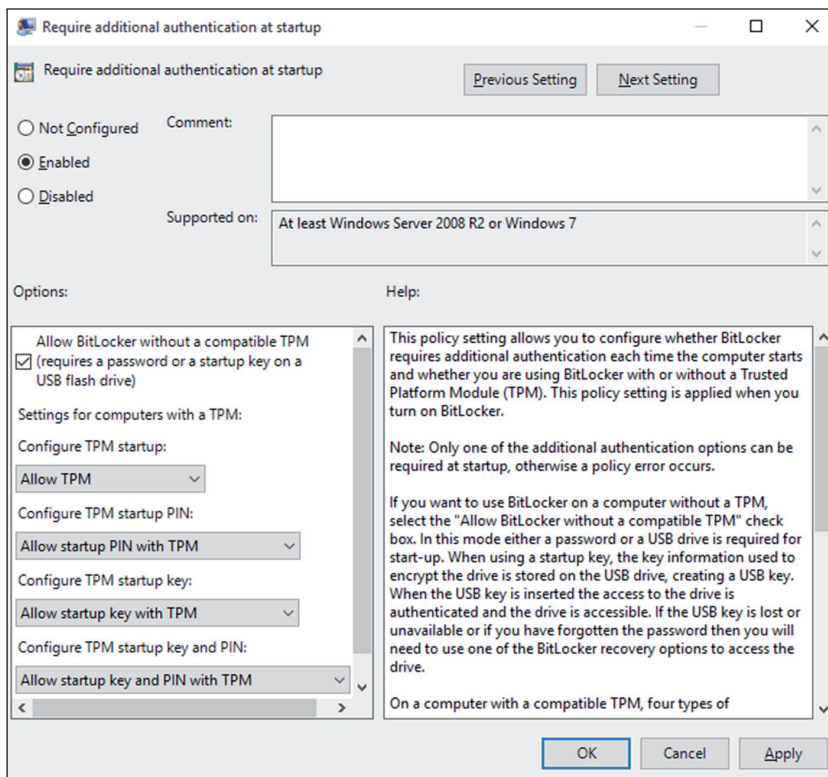
If the TPM discovers a potential security risk, such as a disk error or changes made to BIOS, hardware, system files, or startup components, the system drive will not be unlocked until you enter the 48-digit BitLocker recovery password or use a USB drive with a recovery key as a recovery agent.

BitLocker must be set up either within the Local Group Policy editor or through the BitLocker icon in Control Panel. One advantage of using BitLocker is that you can prevent any unencrypted data from being copied onto a removable disk, thus protecting the computer.

BitLocker Recovery Password

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.

Features of BitLocker

As with any version of Windows, Microsoft continues to improve on technologies for Windows Server 2012 R2 and Windows 10. The following sections cover some of the features of BitLocker.

BitLocker Provisioning

In previous versions of BitLocker (Windows 7), the BitLocker provisioning (system and data volumes) was completed during the post-installation of the BitLocker utility. The BitLocker provisioning was done either through the command-line interface (CLI) or Control Panel. In the Windows 8, Windows 10, and Windows Server 2012 R2 version of BitLocker, an administrator can choose to provision BitLocker before the operating system is even installed.

Administrators have the ability to enable BitLocker, prior to the operating system deployment, from the Windows Preinstallation Environment (WinPE). BitLocker is applied to the formatted volume, and BitLocker encrypts the volume prior to running the Windows setup process.

If an administrator wants to check the status of BitLocker on a particular volume, the administrator can view the status of the drive in either the BitLocker Control Panel applet or Windows Explorer.

Encrypting Used Disk Space Only

Windows 10 BitLocker has a requirement that all data and free space on the drive has to be encrypted. Because of this, the encryption process can take a very long time on larger volumes. In Windows 10 BitLocker, administrators have the ability to encrypt either the entire volume or just the space being used. When you choose to encrypt the Used Disk Space Only option, only the section of the drive that has data will be encrypted. Because of this, encryption is completed much faster.

Standard User PIN and Password Change

One issue that BitLocker has had is that you need to be a local administrator to configure BitLocker on operating system drives. This can be an issue in a large organization due to the fact deploying the Trusted Platform Module (TPM) + PIN to a large number of computers can be very challenging.

Even with the new operating system changes, administrative privileges are still needed to configure BitLocker, but now your users have the ability to change the BitLocker PIN for the operating system or change the password on the data volumes.

When a user gets to choose their own PIN and password, they normally choose something that has meaning and something easy for them to remember. That is a good thing and a bad thing. It's good because when your users choose their own PIN and password, normally they don't need to write it down—they just know it. It's bad because if anyone knows the user well, they can have an easier time figuring out the person's PIN and password. Even when you allow your users to choose their own PIN and password, make sure you set a GPO to require password complexity.

Network Unlock

One of the new features of BitLocker is called Network Unlock. *Network Unlock* allows administrators to easily manage desktop and servers that are configured to use BitLocker. Network Unlock allows an administrator to configure BitLocker to unlock automatically an encrypted hard drive during a system reboot when that hard drive is connected to their trusted corporate environment. For this to function properly on a system, there has to be a DHCP driver implementation in that system's firmware.

If your operating system volume is also protected by the TPM + PIN protection, the administrator has to be sure to enter the PIN at the time of the reboot. This protection can actually make using Network Unlock more difficult to use, but they can be used in combination.

Support for Encrypted Hard Drives for Windows

One of the new advantages of using BitLocker is *Full Volume Encryption (FVE)*. BitLocker provides built-in encryption for Windows data files and Windows operating system files. The advantage of this type of encryption is that encrypted hard drives that use *Full Disk Encryption (FDE)* get each block of the physical disk space encrypted. Because each physical block gets encrypted, it offers much better encryption. The only downside to this

is because each physical block is encrypted, it adds some degradation to the hard drive speed. So, as an administrator, you have to decide if you want better speeds or better security on your hard disk.

Windows 7 and 2008 R2 vs. Windows 10 and 2012 R2

When reading a book on a new operating system, the first question most of us have is what's the difference between Windows 7 and Windows 2008 R2 versus Windows 10 and Windows Server 2012 R2. Table 4.3 shows you many of the common features and how they worked then and now.

TABLE 4.3   BitLocker then and now

Feature	Windows 7/Server 2008 R2	Windows 10/Server 2012 R2
Reset the BitLocker PIN or password	The user's privileges must be set to an administrator if you want to reset the BitLocker PIN on an operating system drive and the password on a fixed or removable data drive.	Standard users now have the ability to reset the BitLocker PIN and password on operating system drives, fixed data drives, and removable data drives.
Disk encryption	When BitLocker is enabled, the entire disk is encrypted.	When BitLocker is enabled, users have the ability to choose whether to encrypt the entire disk or only the used space on the disk.
Hardware Encrypted Drive support	Not supported.	If the Windows logo hard drive comes pre-encrypted from the manufacturer, BitLocker is supported.
Unlocking using a network-based key to provide dual-factor authentication	Not available.	If a computer is rebooted on a trusted corporate wired network, the key protector then allows a key to unlock and skip the PIN entry.
Protection for clusters	Not available.	Windows Server 2012 R2 BitLocker includes the ability to support cluster shared volumes and failover clusters as long as they are running in a domain that was established by a Windows Server 2012 R2 domain controller with the Kerberos Key Distribution Center Service enabled.

TABLE 4.3   BitLocker then and now *(continued)*

Feature	Windows 7/Server 2008 R2	Windows 10/Server 2012 R2
Linking a BitLocker key protector to an Active Directory account	Not available.	BitLocker allows a user, group, or computer account in Active Directory to be tied to a key protector. This key protector allows a protected data volumes to be unlocked.

In Exercise 4.3, you will enable BitLocker on the Windows 10 system.

EXERCISE 4.3

Using BitLocker in Windows 10

1.   Right-click the Start button and choose Control Panel.

2.   Change the View By: Category to Large Icons by using the pull-down menu.

3.   Choose the BitLocker Drive Encryption icon, as shown in Figure 4.21.

   FIGURE 4.21   Choosing the BitLocker icon
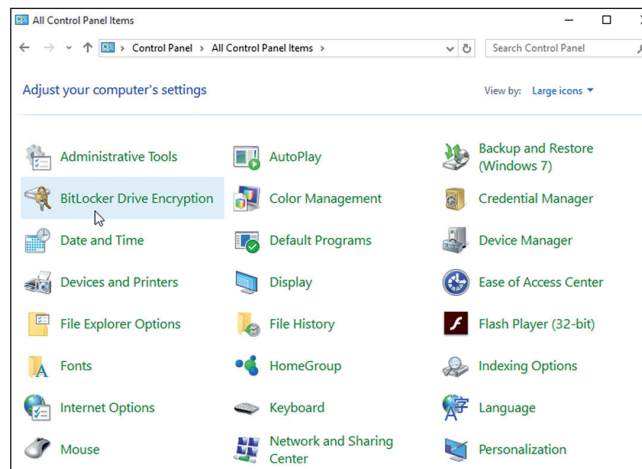
4.   Click the link that says "Turn on BitLocker."

5.   On the Choose How To Unlock The Drive screen, click the "Enter a password" link.

6.   Enter a password, reenter the password, and click the Next button.

7. Pick one of the options on the How Do You Want To Save The Recovery Key screen, and then click Next.

8. On the Choose How Much You Want To Encrypt screen, choose to encrypt used disk space or the entire drive. I am choosing the entire drive.

9. On the Are You Ready To Encrypt The Drive? screen, click Continue.

    The drive will be encrypted. You can unencrypt the drive at any time by choosing Unencrypt Drive from the BitLocker icon in Control Panel.

Using the BitLocker Administration and Monitoring Utility

Microsoft BitLocker Administration and Monitoring (MBAM) is part of the Microsoft Desktop Optimization Pack (MDOP) and will allow the IT department to use enterprise-based utilities for managing and maintaining BitLocker and BitLocker To Go. As I talked about BitLocker, one of the hardest components of BitLocker is managing and maintaining BitLocker deployment and key recovery. This is where MBAM comes in to play.

MBAM helps IT departments simplify BitLocker deployment and key recovery while also providing centralized compliance monitoring and reporting. MBAM also helps minimize the money related to provisioning and supporting encrypted BitLocker drives.

As explained, BitLocker helps protect against the theft of hardware, and MBAM helps an IT department administer BitLocker in an easy-to-use administrative Microsoft Management Console (MMC) interface.

Overview of MBAM

Microsoft has created MBAM 2.5 to help administrators handle and administer BitLocker and BitLocker To Go. MBAM offers many of the following features:

- Allows IT administrators to automatically set up client computers to use encrypted volumes across the entire enterprise.

- Allows corporate security personnel to rapidly determine if the corporate compliances have been met, and it also allows them to check the state of individual computers throughout the network.

- IT members can use Microsoft System Center Configuration Manager to have a centralized reporting and hardware management utility that works with MBAM.

- Helps IT departments to rapidly assist end users with BitLocker PIN and recovery key requests.

- Allows corporate users to recover their own encrypted devices by using the MBAM Self-Service Portal.

- Give corporations piece of mind that their users can work anywhere in the world with the knowledge that corporate data is being protected.

> MBAM is part of the Microsoft Desktop Optimization Pack (MDOP) down-loadable utility, but your network must meet certain requirements. Many of these requirements require server installations and are beyond the scope of this book. To learn more about MBAM, go to the following Microsoft website to see all of the requirements:
>
> https://technet.microsoft.com/en-us/library/mt427465.aspx

Understanding Smart Cards

Another way to help secure Windows 10 is by using smart cards. *Smart cards* are plastic cards (the size of a credit card) that can be used in combination with other methods of authentication. This process of using a smart card along with another authentication method is called two-factor authentication or *multifactor authentication*. Authentication is the process of using user credentials to log on to either a local Windows 10 machine or a domain.

Smart card support allows you to increase the security of many critical functions of your company, including client authentication, interactive logon, and document signing.

Smart cards are now easier than ever to use and deploy because of the new features included with all versions of Windows 10.

Enhanced Support for Smart Card–Related Plug and Play and the Personal Identity Verification (PIV) Standard   This allows users of Windows 10 to use smart cards from vendors who publish their drivers through Windows Update, allowing Windows 10 to use the smart card without special middleware. These drivers are downloaded in the same way as drivers for other Windows devices are downloaded. When a smart card that is PIV compliant is placed into a smart-card reader, Windows 10 will try to download a current driver from Windows Update. If a driver is not available, the PIV-compliant minidriver that is included with Windows 10 is used for the smart card.

Encrypting Drives with BitLocker   If your users are using Windows 10 Enterprise or Professional, the users can choose to encrypt their removable media by turning on BitLocker and then choosing the smart-card option to unlock the drive. Windows will then retrieve the correct minidriver for the smart card and allow the operation to complete.

Smart-Card Domain Logon   When using Windows 10, the correct minidriver for a smart card is automatically retrieved. This allows a new smart card to authenticate with the domain controller without requiring the user to install or configure additional middleware.

Document and Email Signing   Windows 10 users can use smart cards to sign an email or document. XML Paper Specification (XPS) documents can also be signed without additional software.

Use with Line-of-Business Applications   Using Windows 10 smart cards allows applications that use Cryptography Next Generation (CNG) or CryptoAPI to retrieve the correct minidriver at runtime. This eliminates the need for middleware.

Summary

In this chapter, we started looking at how to set up and configure folders on a Windows 10 and Windows Server 2012 R2 system. We talked about sharing those folders and how to grant access to those folders by using NTFS and shared permissions.

We also talked a Dynamic Access Control (DAC) and how Dynamic Access Control allows an administrator to identify data by using data classifications and then controlling access to these files based on these classifications.

DAC also gives administrators the ability to control file access by using a central access policy. This central access policy will also allow an administrator to set up audit access to files for reporting and forensic investigation.

We also talked about BitLocker and BitLocker To Go including Data Recovery Agent and Microsoft BitLocker Administration and Monitoring (MBAM).

We then finished the chapter by talking about two-factor authentication using smart cards. Smart cards and user accounts will be discussed in greater detail in Chapter 8 "Managing Identity and Authorization."

Video Resources

There are videos available for the following exercises:

    4.1

    4.3

You can access the videos at `www.wiley.com/go/sybextestprep` on the Other Study Tools tab.

Exam Essentials

Understand folder options.   Understand the purpose and features of using folders and files. Properly configuring folders and folder access is one of the most important tasks that we do on a daily basis.

Understand NTFS and share permissions.   Be able to configure security permissions and know the difference between NTFS and share permissions.

Know how to use BitLocker Drive Encryption.   Understand the purpose and requirements of BitLocker Drive Encryption. Know which editions of Windows 10 (Enterprise, Education, and Professional) include BitLocker.

Understand Microsoft BitLocker Administration and Monitoring (MBAM).   Understand the purpose and requirements of MBAM. MBAM allows an IT department to manage all of your BitLocker setting through the use of one application.

Understand Smartcards.   You need to understand smart cards and two-factor authentication. The reason it is called two-factor authentication is because you need the smart card and the PIN (two factors).

Review Questions

1. You are hired by a friend to set up a network in their home. They have four machines in their home that are all connected by an ISP wireless router. The systems can't share documents because there is currently no network sharing in place. They want to be able to share audio and video files among their family. How can you easily set up a network? Choose two.

A. Install a Windows Server 2008 R2 domain controller.

B. Create a HomeGroup.

C. All audio and video files should be moved to the HomeGroup libraries.

D. Move all audio and video files to a shared folder on the Windows Server 2008 R2 machine.

2. You are the network administrator for a large organization. You have a Windows 10 machine that needs to prevent any user for copying unencrypted files from the Windows 10 machine to any removable disk. How do you accomplish this task?

A. Within the System icon in Control Panel, set the BitLocker Drive encryption.

B. Within the Hardware icon in Control Panel, set the BitLocker Drive encryption.

C. Within the Device Manager icon in Control Panel, set the BitLocker Drive encryption.

D. Within a Local Group Policy, set the BitLocker Drive encryption.

3. Which editions of Windows 10 can you enable BitLocker? Choose all that apply.

A. Windows 10 Education Edition

B. Windows 10 Basic Edition

C. Windows 10 Professional Edition

D. Windows 10 Enterprise Edition

4. You have a network folder that resides on an NTFS partition on a Windows 10 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.

5. 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.

6. Jeff, the IT manager for Stormwind, has been asked to give Tom the rights to read and change documents in the `Stormwind Documents` folder. The following table shows the current permissions on the shared folder:

Group/User	NTFS	Shared
Sales	Read	Change
Marketing	Modify	Change
R&D	Deny	Full Control
Finance	Read	Read
Tom	Read	Change

Tom is a member of the Sales and Finance groups. When Tom accesses the `Stormwind Documents` folder, he can read all the files, but the system won't let him change or delete files. What do you need to do to give Tom the minimum amount of rights to do his job?

   A. Give Sales Full Control to shared permissions.

   B. Give Tom Full Control to NTFS security.

   C. Give Finance Change to shared permissions.

   D. Give Finance Modify to NTFS security.

   E. Give Tom Modify to NTFS security.

7. You are the IT manager for your company. You have been asked to give the Admin group the rights to read, change, and assign permissions to documents in the `Stormwind Documents` folder. The following table shows the current permissions on the `Stormwind Documents` shared folder:

Group/User	NTFS	Shared
Sales	Read	Change
Marketing	Modify	Change
R&D	Deny	Full Control
Finance	Read	Read
Admin	Change	Change

What do you need to do to give the Admin group the rights to do their job? (Choose all that apply.)

A. Give Sales Full Control to shared permissions.

B. Give Full Control to NTFS security.

C. Give Admin Full Control to shared permissions.

D. Give Finance Modify to NTFS security.

E. Give Admin Full Control to NTFS security.

8. Vincent is an instructor for Stormwind, and he is talking to Jeff, the company's IT manager. Vince asks Jeff to implement some type of two-factor authentication. What can Jeff install to complete this request?

A. Passwords and usernames

B. Retina scanners

C. Fingerprint scanners

D. Smart cards

9. You are using Windows 10 and you have created a file with called "my text" in Notepad and has a `.txt` extension type. You need to change the extension type from `.txt` to `.vbx`. What setting do you need to change on the folder so that you can see the extension types?

A. Uncheck Hide Extensions For Known File Types

B. Check Unhide Extensions For Files

C. Check show Extensions For Files

D. Uncheck Hide All File Types

10. The owner of your company has come to you and stated that they want all of the hardware on all systems to use BitLocker and BitLocker To Go. What utility should you install to help manage and maintain BitLocker and BitLocker To Go?

A. MAAM

B. MBAM

C. MNBM

D. MABM

Chapter

5

Managing the Windows 10 Environment

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Configure mobility options.**

- This objective may include but is not limited to the following subobjectives: Configure offline file policies, configure power policies, configure Windows To Go, configure sync options, configure Wi-Fi direct, files, powercfg, Sync Center.

✓ **Configure remote connections.**

- This objective may include but is not limited to the following subobjectives: Configure remote authentication, configure Remote Desktop settings, configure VPN connections and authentication, enable VPN reconnect, configure broadband tethering.

After you've installed Windows 10, you will need to configure the system. In this chapter, we will examine the process of configuring the Windows 10 environment, beginning with an overview of the main configuration utilities.

Control Panel is one of the most important configuration tools for Windows 10. It includes many icons that can help you optimize, maintain, and personalize the operating system. One of the most important icons in Control Panel is the System icon. The System icon not only has operating-system information, but it also allows you to configure devices, remote settings, and system protection.

If you use Windows 10 on a laptop computer, it is important to properly configure your power and mobility options. Configuring these options on a laptop will allow you to get the most out of your laptop and Windows 10. There are many different mobility options that you can choose from to help customize the laptop to each individual user.

We will also examine how services operate and how to configure your services to start manually or automatically. We will examine how to configure services in the event of a service error.

Configuring the Windows 10 Operating System

After Windows 10 is installed, the next important step is configuration. If a Windows 10 machine is not configured properly, it may not run properly. When you are the IT administrator for a company, you need to make sure that the Windows client systems are configured properly and, in most cases, the same.

There are many ways to do this, from individually configuring the Windows 10 systems to using Group Policy Objects (GPOs). Most companies are going to set Windows 10 configurations through the use of Windows Servers and GPOs, but you still need to understand each component and what it does so you can configure the proper settings.

The following sections describe many of the configuration options for customizing Windows 10 for each user's needs. We will start with configuring the Windows 10 desktop environment.

Configuring the Desktop Environment

The Windows 10 desktop is the interface that appears when a user logs into the operating system. The desktop includes the wallpaper, Start menu, tiles, and icons (see Figure 5.1).

FIGURE 5.1   The default Windows 10 desktop
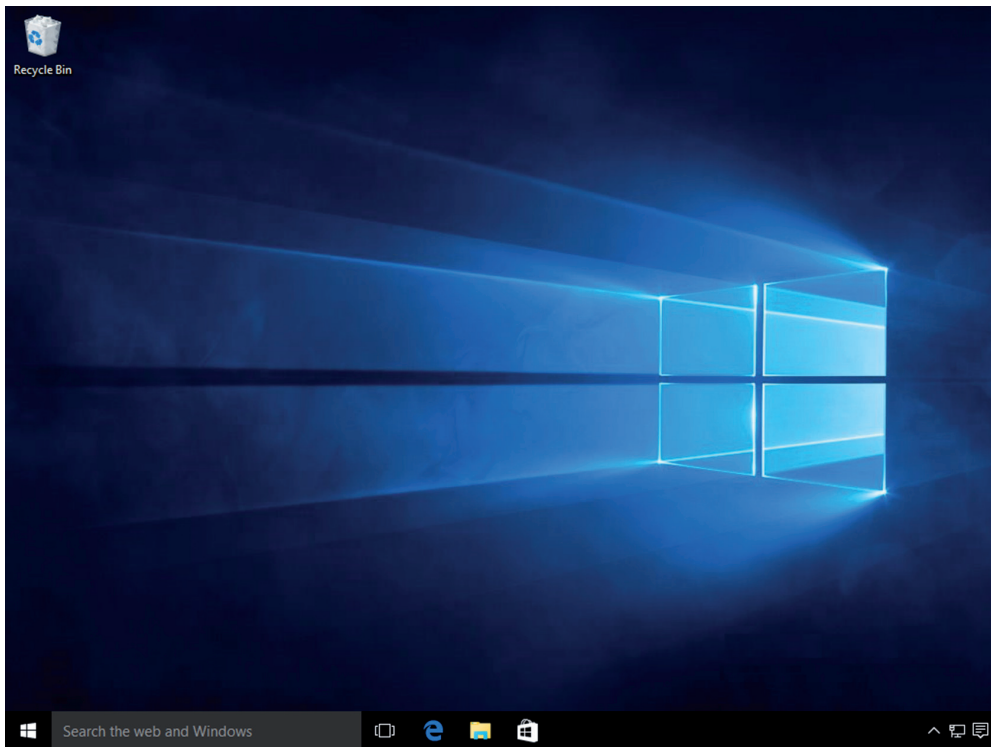
The Windows 10 Start menu, located at the bottom left of the desktop by default, includes the default All Apps section shown in Figure 5.2.

FIGURE 5.2   The All Apps section
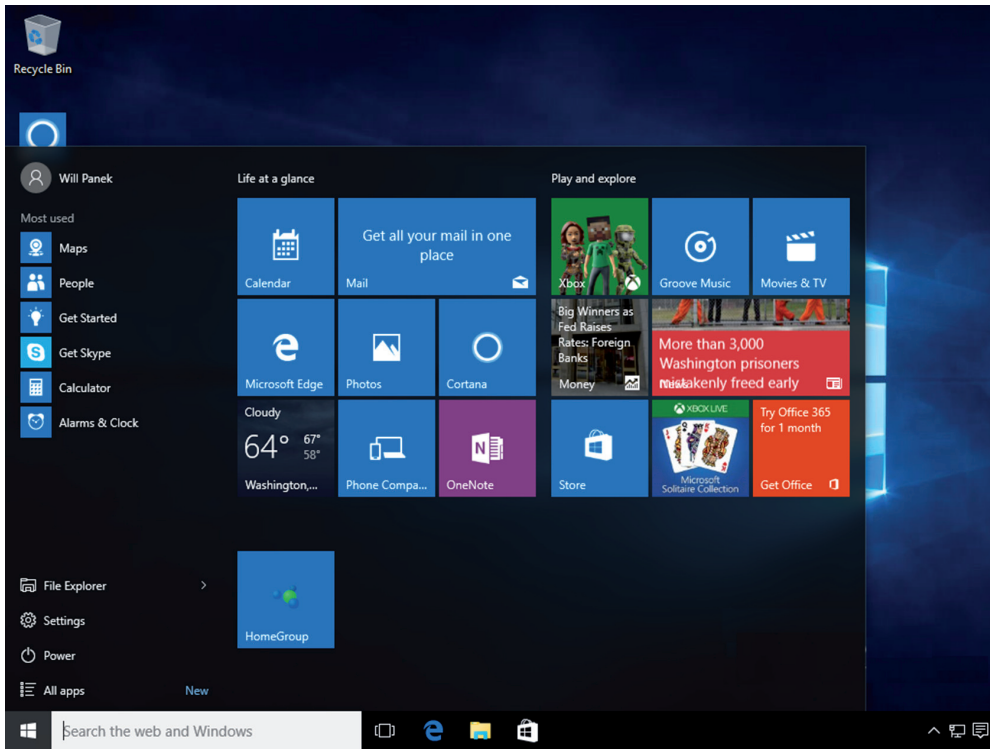
The Windows 10 default desktop appears after a user has logged onto a Windows 10 computer for the first time. When you install a new instance of Windows 10, you will notice that the desktop is clean except for the Recycle Bin. You may also have a message on the desktop that states that the Windows 10 system has not been activated (as shown in Figure 5.3).

Users can then configure their desktops to suit their personal preferences and to work more efficiently. The following list describes some of the common default options that appear on the Start menu, in the Most Used section, Control Panel, and All Apps section. This list includes some of the more commonly used applications and shortcuts; it's not a complete list of every application available to you.

> **NOTE**   Depending on which version of Windows 10 you are using, these options may vary a bit.

FIGURE 5.3   The desktop with activation notice

Windows Applications

The following are some of the applications for Windows 10. These are not all of the applications installed by default on Windows 10 but just a few to get you started.

Calculator   This shortcut starts the Calculator program. The Calculator works like any other store-bought calculator, and it can even be changed from a Standard calculator to a Scientific, Programmer, Converter, Volume, Length, Weight & Mass, or Temperature calculator.

Cortana   With this application, you can speak or type into the Windows 10 system, and your personnel assistant, Cortana, will try to find answers to any queries that you may have.

Getting Started   This is used to access preset tasks. Some of these tasks are Get To Know Windows 10 (see Figure 5.4), Microsoft Edge, Start Menu Tips, Setting Things Up, Get Connected, Cortana, Windows Hello, XBOX App, Entertainment, Office, Personalize And Settings, Saving And Syncing Content, Apps And Store, Continuum And Touch, and Ease Of Use.

FIGURE 5.4 Getting Started tasks
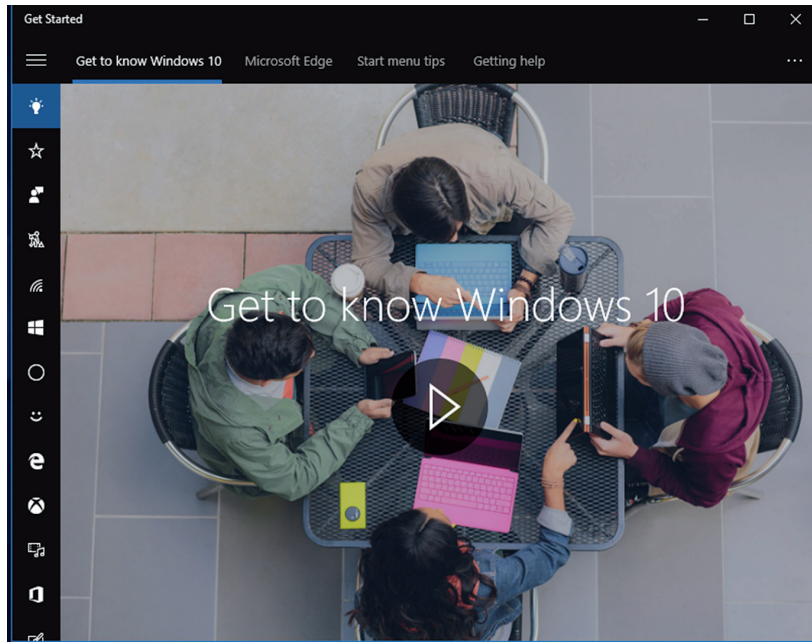
Get Skype This app allows you to download and configure Skype. If your company uses Skype, Windows 10 gives you the ability to download and set up your Skype account with the Windows 10 operating system.

Maps This app allows you to see the current location and area of the Windows 10 system. You can use Maps to search for locations and services (food, gas, directions, etc.), as shown in Figure 5.5.

Microsoft Edge This shortcut starts the built-in web browser. When used with an Internet connection, Microsoft Edge provides an interface for accessing the Internet or a local intranet.

OneDrive This application allows you to connect with the Microsoft OneDrive cloud-based utility. You can use this application to share documents between the Windows 10 system and the OneDrive cloud-based subscription.

People This application allows you to look up and work with your contacts. It enables you to use social media to connect people and contacts.

Windows Update This shortcut allows you to receive updates and security patches for the Windows 10 operating system. You can receive updates from either Microsoft's web server or a Windows Server Update Services (WSUS) machine.

FIGURE 5.5   Maps
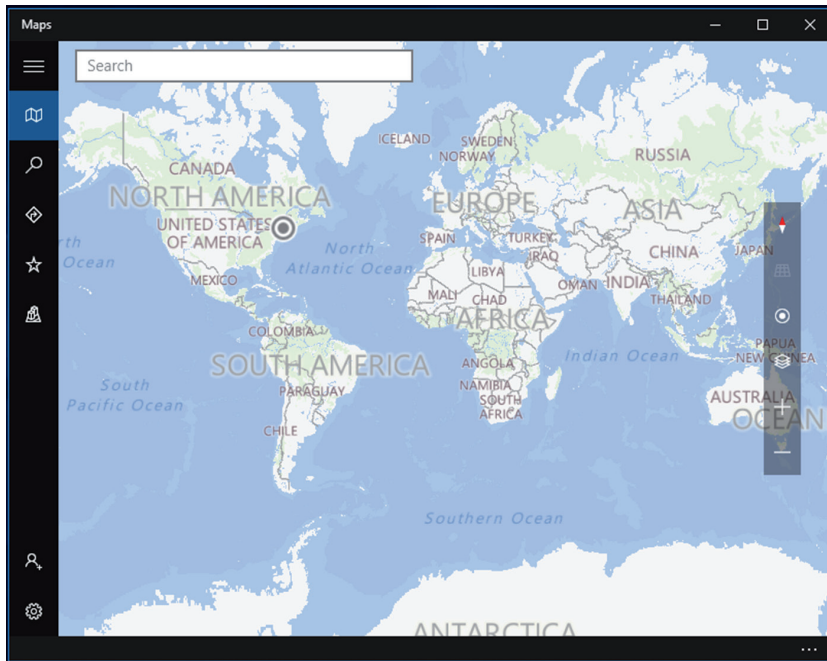
XPS Viewer   This application allows you to view Microsoft XML Paper Specification
(.xps) files. The XPS viewer also allows you to print these files.

Windows Accessories

Windows Accessories are some basic tools that are included with Windows 10 to help you
do tasks from surfing the net to playing DVDs.

Internet Explorer   This shortcut starts the built-in web browser. When used with an
Internet connection, Internet Explorer provides an interface for accessing the Internet or a
local intranet.

Microsoft Edge   There is another Internet browser on Windows 10 called Edge. Microsoft
Edge gives you new ways to find pages, read and write on the Web, plus help from Cortana
when you need it.

Notepad   This application allows you to create text files. This is a great way to store notes
on the Windows 10 system without using a full word processing application like Word.

Paint   This shortcut starts the Paint program. The Paint program is an application that
allows you to change or manipulate graphics files.

Remote Desktop Connection This program allows a user to connect remotely to another machine. To connect to another computer, Remote Desktop Connection must be enabled on the receiving computer.

Snipping Tool This tool allows a user to capture an item on the desktop (see Figure 5.6). The user clicks the Snipping Tool and drags the cursor around an area that will then be captured. The captured area can then be drawn on, highlighted, or saved as a file.

FIGURE 5.6 Snipping Tool
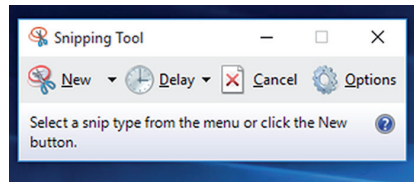
Sticky Notes This application places a sticky note on the desktop, as shown in Figure 5.7. You can then type a message or reminder into the sticky note. It will remain on the desktop until you delete it.

FIGURE 5.7 Sticky Notes application
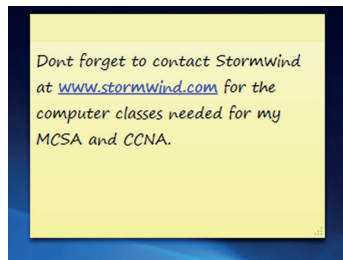
Settings This application opens the Settings window. Inside the Settings window, you can configure your System, Devices, Network & Internet, Personalization, Accounts, Time & Language, Ease Of Access, Privacy, and Updates & Security (see Figure 5.8).

Store This application allows you to download and purchase applications from the Microsoft Store. The Microsoft Store has thousands of business and personnel applications that you can use on Windows 10.

Windows Fax And Scan This application allows you to create and manage scans and faxes. Windows Fax And Scan allows users to send or receive faxes from their workstation.

FIGURE 5.8 Settings window
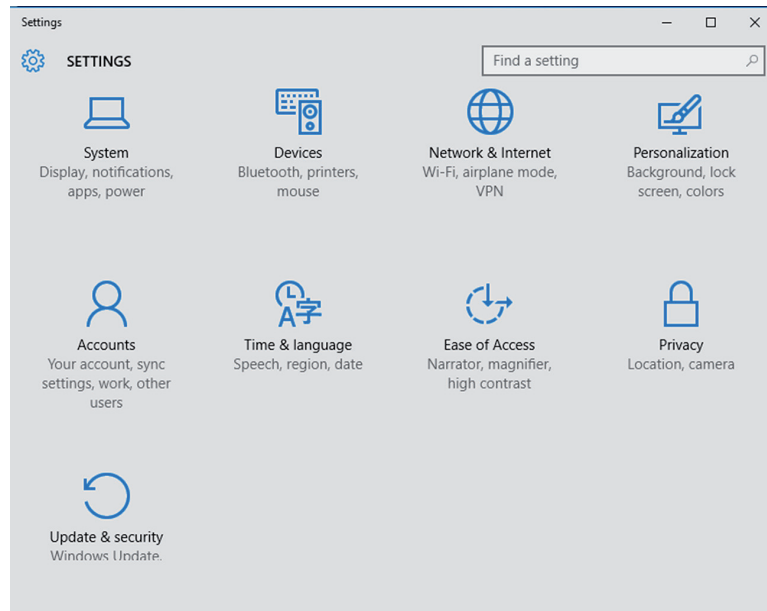
Windows Media Player With this application, you can play all your media files, including videos, music, pictures, and recorded TV.

Windows Ease Of Access Tools

These tools are installed on a Windows 10 system to help individuals who have difficulty seeing the screen. The Ease Of Access tools can be accessed via Start ➤ All Apps ➤ Ease of Access and include a Magnifier, Narrator, On-Screen Keyboard, and Windows Speech Recognition, as shown in Figure 5.9.

FIGURE 5.9 Ease Of Access tools
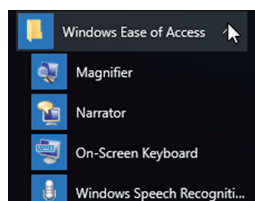
Windows System Utilities

These utilities are the ones that help most IT administrators manage and control Windows systems. These are the tools that help us start, manage, and control the Windows 10 systems and applications.

Command Prompt   The Command Prompt is one of the most useful utilities to an IT administrator. You can run commands through the Command Prompt and program the Windows 10 system using system commands.

Control Panel   Control Panel holds many utilities and tools that allow you to configure your computer. It is discussed in greater detail later in this chapter.

Default Programs   When you choose the Default Programs shortcut, four different configuration items can be accessed (as shown in Figure 5.10): Set Your Default Programs, Associate A File Type Or Protocol With A Program, Change AutoPlay Settings, and Set Program Access And Computer Defaults. Each of these allows you to change the default programs that are used within Windows 10.

FIGURE 5.10   Default Programs
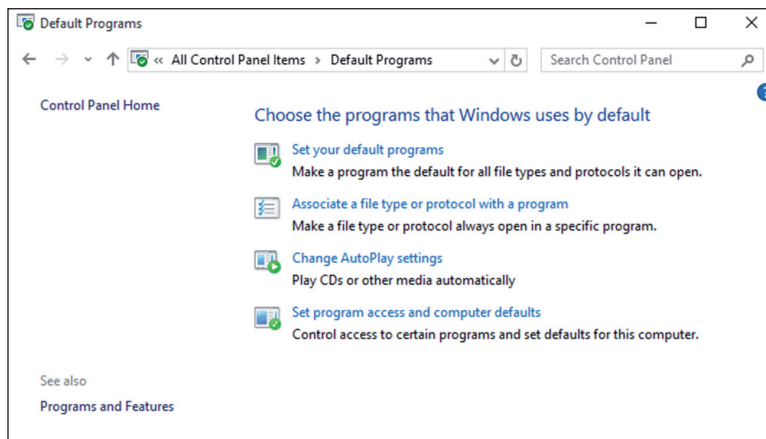
Devices   This shortcut opens the Devices section, where you can add or configure any of your hardware devices.

File Explorer   By default, this application shows all of the folders and files that are on the Windows 10 system. You can use this application to look at all of the files located on the Windows 10 system.

Run   You can either put in commands or run applications from the Run dialog box.

Task Manager   This is one of the few applications that I used as an IT director on a daily basis. The Task Manager allows you to see what applications are running on the Windows

systems (including servers). The Task Manager also allows you to stop applications from running on a system. This utility will be explained in greater detail throughout this book.

This PC   This shortcut allows you to centrally manage your computer's files, hard drives, and devices with removable storage. It also allows you to manage system tasks and other places and to view details about your computer.

Windows User's Tools

The Windows User's tools are the utilities we use to store and access user's data and documents. These are the applications and folders that we use to keep user data.

Desktop   This folder shows all of the applications that are located on the desktop.

Documents   By default, this folder stores the documents that are created. Each user has a unique Documents folder, so even if a computer is shared, each user will have his or her own personal folder.

Pictures   This application shows any pictures that are in the user's Pictures folder.

Music   This shortcut will show any music that is in the Music folder.

Videos   This shortcut shows you all of the videos that are stored on this Windows 10 system.

Shut Down or Restart   This button is used to shut down or restart the computer. There is an arrow next to the button that you can use to restart the machine or shut down the system.

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. You can restore or permanently delete a file from the Recycle Bin by opening the Recycle Bin and right-clicking that file.

When configuring the desktop, you have the ability to decide between configuring a background of your choice as your desktop backdrop or you can choose one of the built-in desktop themes. Desktop themes are a preset package containing graphical appearance details, used to customize the look and feel of an operating system.

Backgrounds are just the graphics that you decide to set as your wallpaper. To switch between different themes, right-click an area of open space on the desktop and select Personalize. In the Theme Settings dialog box, you can select the theme you want to use. You can additionally configure the desktop by customizing the taskbar and Start menu, adding shortcuts, and setting display properties.

Configuring Personalization

To configure the Windows desktop and how it looks, right-click the Desktop and selecting Personalize. When you choose to Personalize the desktop, you have five different settings that you can configure (as shown in Figure 5.11).

FIGURE 5.11 Personalization screen
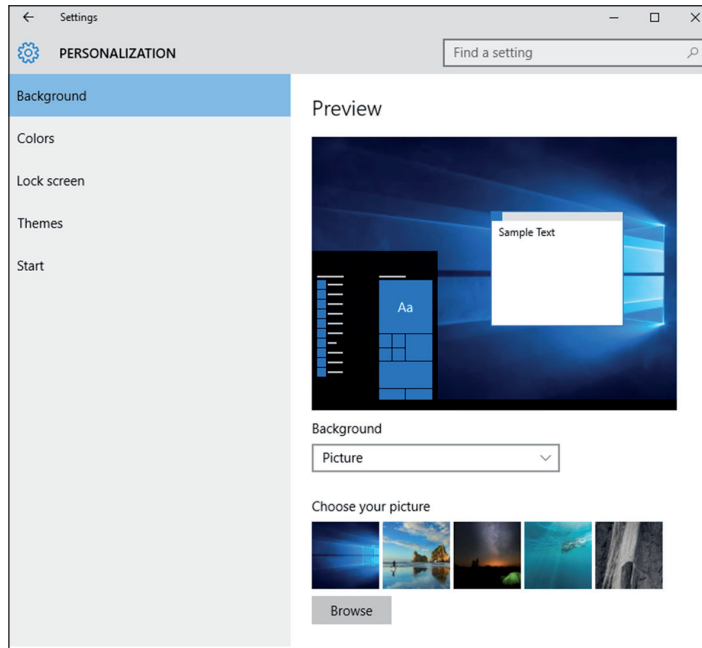
Background

This lets you pick your desktop background, which uses a picture or an HTML document as wallpaper. Setting up a desktop background can be as easy as picking a solid color and placing a picture of your favorite sports team or pet on top of it.

Windows 10 comes with some pictures already in the system, but you can basically turn any picture into your background desktop picture. As you can see in Figure 5.11, you can click the Browse button and choose the pictures that you want in your background.

Colors

This allows you to fine-tune the color and style of your windows background and accent. Windows 10 gives you the ability to automatically pick an accent color for your background, as shown in Figure 5.12.

Windows 10 users also have the ability to automatically choose their own background colors. You can show colors on the Start screen, taskbar, and action center. You can also make the Start screen, taskbar, and action center transparent.

FIGURE 5.12   Colors screen
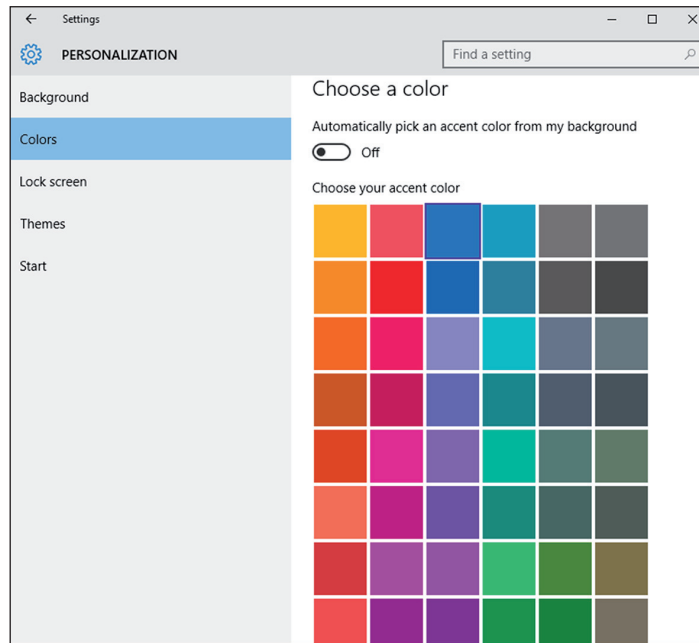
Lock Screen

This lets you select a screen saver that will start after the system has been idle for a speci-fied amount of time. You can also specify a password that must be used to access the system after it has been idle. When the idle time has been reached and the screen saver is activated, the computer can also be set so that the Windows 10 system is locked (shown in Figure 5.13) and the password (or other authentication method) of the user who is currently logged on must be entered to unlock the computer again.

Windows 10 includes many different screen-saver options that can be used and configured:

- None
- 3D Text
- Blank
- Bubbles
- Mystify
- Photos
- Ribbons

FIGURE 5.13 Lock Screen
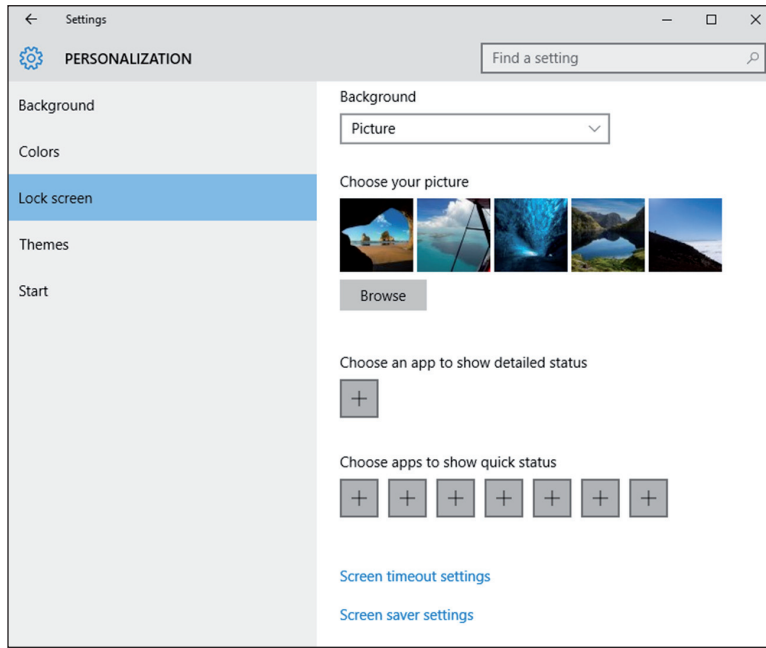
Personalization Themes

This screen allows you to set the different themes that you can have for your desktop. Themes allow you to change the color pattern for all desktop and applications in one setting. The Themes screen (shown in Figure 5.14) also allows you to change the advanced sound settings, desktop icon settings, and mouse pointer settings.

Advanced Sound Settings   This lets you choose the sounds that will be played based on the action taken. Each action can have its own sound. The Sound options also allow you to set up the external or internal speakers and microphones that you want to use. You can also calibrate different pieces of hardware.

Desktop Icon Settings   This allows you to customize the desktop icons. You also have the ability to change shortcut icons. Some of the icons that you can add to the desktop are the Computer icon, User's Files icon, Network icon, Recycle Bin icon, and Control Panel. You also have the ability to change icons at the screen.

Mouse Pointers Settings   This allows you to customize the appearance of the mouse pointers. It allows you to go from the traditional pointer to a Help Select, Busy, and Precision Select to just name a few. You can also change the Button options, Pointer Options, Wheel options, and Hardware.
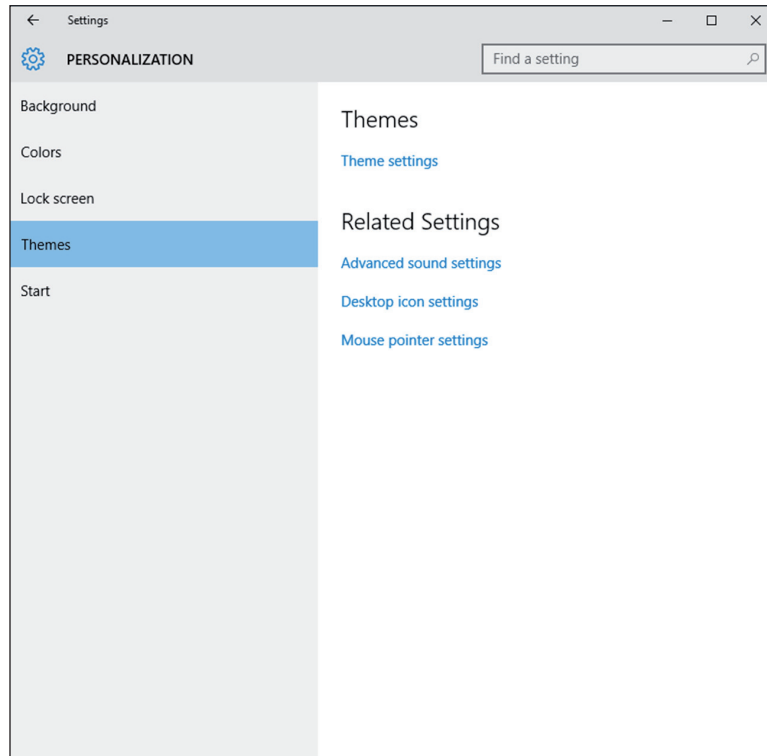
Personalization Start Screen

The Start section allows you to configure what you going to see on your Start menu and which folders appear on the Start. As you can see in Figure 5.15, you have the ability to set the following settings;

- Show most used apps
- Show recently added apps
- Use Start full screen
- Show recently opened items in Jump Lists on Start or the taskbar
- Choose which folders appear on Start

Now that we have looked at how to configure the Windows 10 desktop, let's go ahead and practice doing just that. Exercise 5.1 will walk you through the process of configuring your theme and choosing additional options.

FIGURE 5.15 Start options
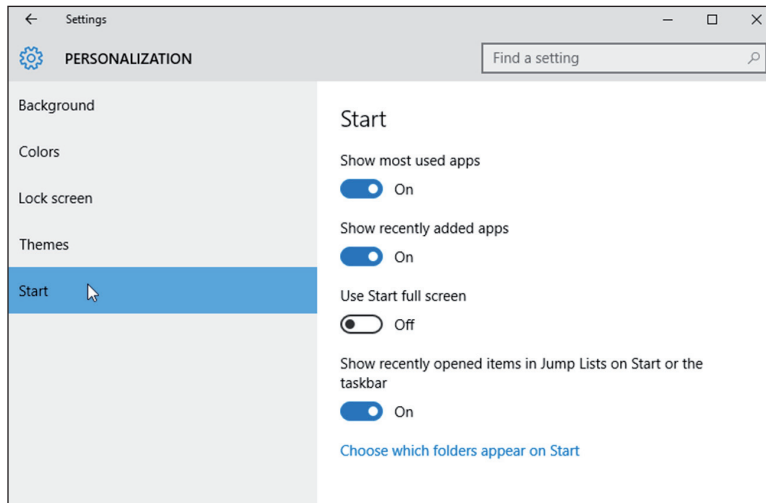
EXERCISE 5.1

Configuring Windows 10 Desktop Options

1. Right-click an open area of the desktop and choose Personalize.

2. On the Background screen, either choose a new picture or use the pull-down under Background and choose Solid Color or Slideshow.

3. After you have set your new desktop, go to the Lock Screen page.

4. Scroll down and choose the link "Screen saver settings."

5. Under the Screen Saver pull-down, choose 3D Text.

6. Click the Setting button. Make sure the radio button is set for Custom Text and put in the text you would like to see. Go ahead and change the font or size or rotation speed. Once completed, click the OK button. At the Screen Saver Settings screen, change the Wait Time to 15 minutes and then click the OK button.

7. Click the Themes screen. Click the Theme Settings link and choose a new theme that you like. You can also keep the current theme if you like that one. Hit the upper-right X to close the window once you're finished.

8. Click the Start screen. Make any changes that you want to change for your Start menu. Once you are finished, close the Personalization window.

⊕ **Real World Scenario**

Configuring Personal Preferences

One thing that I noticed as an IT manager is that the most common configuration change made by users is to configure their desktop. This lets them use the computer more efficiently and often makes them more comfortable with the computer.

To help users work more efficiently with their computers, it's good to 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 seldom used or not used 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 that has been personalized to their preferences. This might include their choice of a desktop theme and screen saver.

Windows 10 includes several utilities for managing various aspects of the operating-system configuration. In the following sections, you will learn how to configure your operating system using Control Panel and the Registry Editor.

We will start with Control Panel and the different utilities included within it.

Using Control Panel

Control Panel is a set of GUI utilities that allow you to configure Registry settings without the need to use a Registry Editor. The Registry is a database used by the operating system to store configuration information.

Let's take a closer look at the utilities that are available through Control Panel. I have set Control Panel to Large Icons view, but you can set it to Small Icons view if you prefer (see Figure 5.16).

> **NOTE**   If you keep the Control Panel view set to Category, you will not be able to follow along and see all the different items we are going to talk about. The Category view has all of these settings, but they are in different sections. I feel it's easier to understand each item using the Large Icons view.

FIGURE 5.16   Control Panel
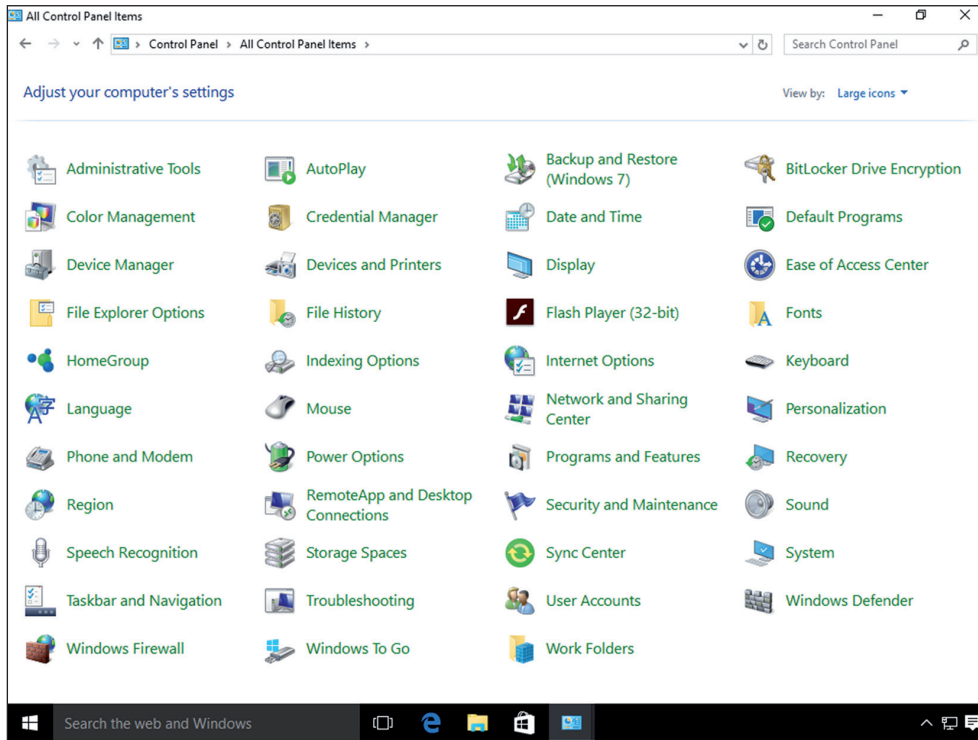
Administrative Tools   This icon has multiple administrative tools that can help you configure and monitor the Windows 10 operating system. These tools include the following:

- Component Services
- Computer Management
- Defragment and Optimize Drives
- Disk Cleanup
- Event Viewer
- iSCSI Initiator
- Local Security Policy
- ODBC Data Sources (32-bit)
- ODBC Data Sources (64-bit)
- Performance Monitor
- Print Management
- Resource Monitor
- Services

- System Configuration
- System Information
- Task Scheduler
- Windows Firewall with Advanced Security
- Windows Memory Diagnostics

AutoPlay   This icon lets you configure media disks and will autoplay when inserted into the media player (see Figure 5.17). Each media type has different configuration settings, but the basic choices are as follows:

- Use AutoPlay for all media and devices
- Removable drive
- Camera Storage
- DVDs
- Blue-ray discs
- CDs
- Software
- Devices

FIGURE 5.17   AutoPlay options
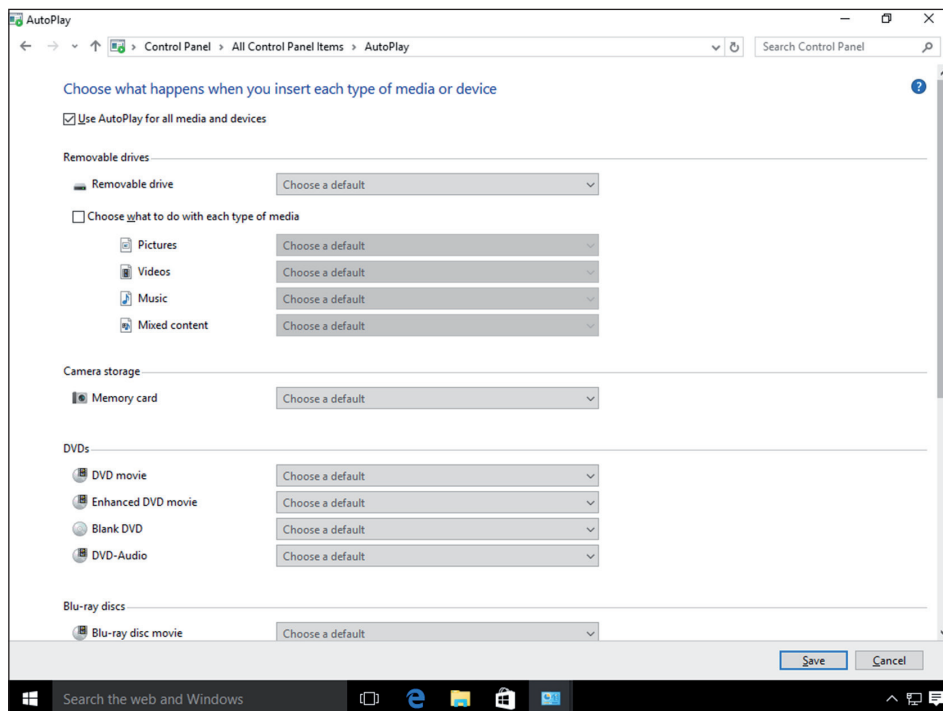
Backup And Restore (Windows 7)   The Backup And Restore icon allows you to configure your backup media. Users can make copies of all important data on their machine to avoid losing it in the event of a hardware failure or disaster. Backups will be discussed in greater detail in Chapter 10, "Configuring Recovery."

BitLocker Drive Encryption   BitLocker Drive Encryption helps prevent unauthorized users from accessing files stored on hard drives by encrypting the drive in its entirety. The user is able to use the computer as they normally would, but unauthorized users cannot read or use any of their files. BitLocker Drive Encryption will be discussed in greater detail in Chapter 6, "Planning and Managing Microsoft Intune."

Color Management   The Color Management icon allows you to configure some of the video adapter's settings. You can configure the Windows color system defaults, the ICC Rendering Intent to WCS Gamut Mapping settings, and the display calibration. You can also change the system defaults to indicate how these items should be handled.

Credential Manager   Users can use the Credential Manager to store credentials such as usernames and passwords. These usernames and passwords get stored in vaults so that you can easily log onto computers or websites.

There are two sections in the Credential Manager: Web Credentials and Windows Credentials. You can add credentials by clicking the link next to each of the two credential sections.

Date And Time   The Date And Time icon allows you to configure your local date and time for the Windows 10 machine. You also have the ability to synchronize your clock with the Internet, as shown in Figure 5.18. Be aware that if your computer is a member of a domain, you will not see this screen and will not be able to synchronize your time with an Internet time server.

FIGURE 5.18   Time synchronization
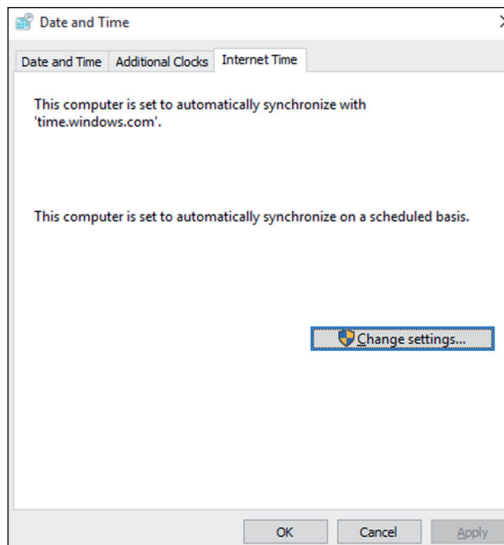
Default Programs   The Default Programs icon allows you to choose the programs that Windows will use by default. For example, you can set Internet Explorer to be the default web browser.

Device Manager   The Device Manager icon allows you to configure the different devices on your Windows 10 machine. You can configure such devices as disk drives, display adapters, DVD/CD-ROM drives, monitors, and network adapters.

Devices And Printers   The Devices And Printers icon lets you add or configure the devices on your machine and your printers. This is where you add the printers that you have on your network.

Display   The Display icon allows you to configure your display. You can change the size of the text and other items on your screen. You also have the ability to change the resolution, calibrate colors, change display settings, adjust ClearType text, and change custom text size.

Ease Of Access Center   The Ease Of Access Center icon allows you to set up your accessibility options.

File Explorer Options   The Folder Options icon allows you to configure how you view folders on the Windows 10 machine by default. You have the ability to set up how you browse and navigate folders, which files and folders you can view (see Figure 5.19), and how folders are searched.

File History   File History allows users to save copies of their files so that you can get them back in the event of a file being lost or damaged. You have the ability to restore personal files, select drives, exclude folders, and even set advanced settings on the File History settings.

FIGURE 5.19   Folder Options
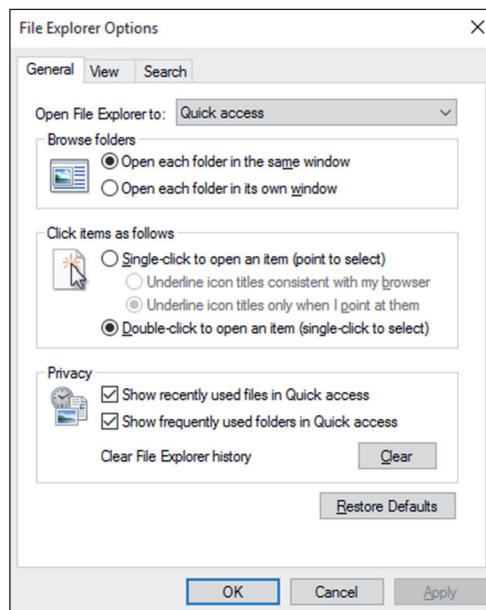
Flash Player (32-bit)   The Flash Player application allows you to set up how your Flash Player is going to operate and which applications the Flash Player will be associated with.

Fonts   This icon displays a screen where you can install, preview, delete, show, hide, and configure the fonts that the applications on your Windows 10 operating system can use. It enables you to get fonts online, adjust cleartext, find a character, and change font size.

HomeGroup   HomeGroups are small local networks that you can easily configure at home. When you install HomeGroups on your first computer, a password is assigned so that you can connect other computers to this HomeGroup. The password can be changed from the HomeGroup icon. HomeGroups are discussed in greater detail in Chapter 9, "Configuring Network Connectivity."

Be aware that if your computer is a member of a domain, you can belong to a HomeGroup that someone else creates but you cannot create your own HomeGroup.

Indexing Options   Windows uses indexing to perform very fast searches of common files on your computer. The Indexing Options feature gives you the ability to configure which files and applications get indexed.

Internet Options   The Internet Options icon allows you to configure how the Internet will operate (see Figure 5.20). From this icon you can configure your home page, browsing history, tabs, security, privacy, content, connections, and programs. Internet Explorer will be discussed in greater detail in Chapter 7, "Configuring Applications."

F I G U R E   5 . 2 0   Internet Properties
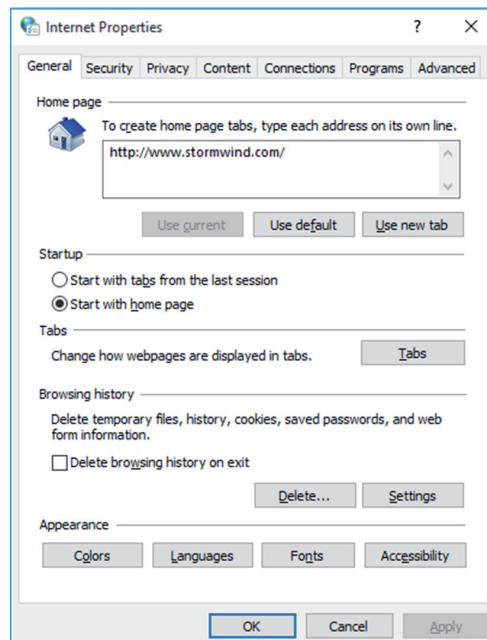
Keyboard   The Keyboard properties allow you to configure how the keyboard will react when used. You can set the character repeat speed (how fast the keyboard will repeat what you are typing) and the cursor speed. You can also use these properties to configure the keyboard drivers.

Language   The Language application allows you to specify which languages you are going to be using on this Windows 10 system. The language at the top of your Language list is the primary language that the system will use.

Mail   You may or may not have this Mail application in Control Panel. If you have a mail client, such as Outlook, then the Mail application icon will be in Control Panel. If you don't have a mail client, then this icon will be missing from Control Panel.

When you configure the Mail properties, you set up your client-side mail settings. In the Mail properties, you can set up different user profiles (mailboxes) and the local mail servers or Internet mail servers to which they connect.

Mouse   Mouse properties give you the ability to configure how the mouse will operate. You can configure the buttons, click speed, ClickLock, pointer type, pointer options, center wheel, and hardware properties.

Network And Sharing Center   The Network And Sharing Center properties configure your Windows 10 machine to connect to a local network or the Internet. You can configure TCP/IP, set up a new network, connect to a network, choose a homegroup, and configure the network adapter. Network And Sharing Center is discussed in greater detail in Chapter 9.

Personalization   Personalization allows you to set up your desktop environment to your liking. Personalization allows you to set up a desktop theme or background, system sounds, screen saver, desktop icons, mouse pointer, and account picture.

Phone And Modem   The Phone And Modem properties are used to set up local dialing properties and modem options. You can set up your dialing location, modem properties, and telephony providers.

Power Options   Power options allow a user to maximize their Windows 10 machine's performance and/or conserve energy. You can enter your own power restrictions to customize your machine. Power options are important settings when you are dealing with laptops. Since many laptops use batteries, power options allow you to get the most time from their batteries. Power management will be discussed later in this chapter.

Programs And Features   The Programs And Features icon was the Add/Remove Programs icon in Windows XP. Programs And Features allows you to organize, uninstall, change, or repair programs and features.

The Programs And Features icon also allows you to choose which Windows 10 features you want installed on the machine, such as Indexing Services, Telnet Client, Telnet Server, and so on.

In Exercise 5.2, you'll install the Telnet client on the Windows 10 operating system.

Installing Features

1. Open the Programs And Features tool by clicking Start ➢ Control Panel ➢ Programs And Features.

2. Click the Turn Windows Features On Or Off link in the upper-left corner.

3. Scroll down the features list and check the Telnet Client check box (shown in Figure 5.21).

F I G U R E 5 . 2 1 Telnet Client check box
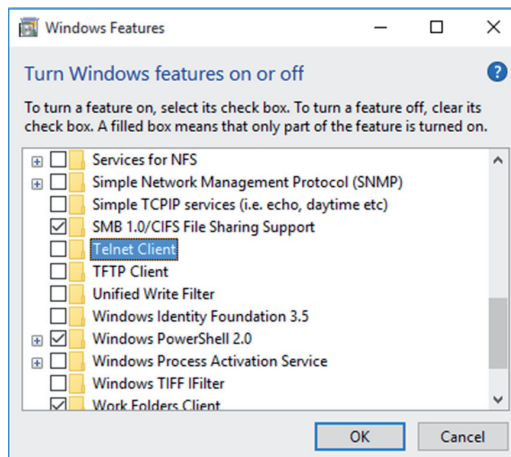
4. Click OK.

🌐 **Real World Scenario**

Using Telnet

As an IT manager, my job does not just consist of working on Windows machines. I also need to understand and work on routers.

You can use the Telnet client to connect to most routers. Using the Telnet client, you can configure the router to operate the way your organization needs it to operate.

I describe Windows Firewall later in this section; however, I do not recommend that you use Windows Firewall as your main line of defense against hackers. You need to purchase a good router/firewall to complete this task. Knowing how to configure the router using the Telnet client will help you accomplish your networking needs.

Recovery   The Recovery icon allows a user or administrator to recover the Windows 10 system to a previously captured restore point. System Restore is one of the first recovery options that should be considered when your Windows 10 system is experiencing problems. Recovery will be discussed in detail in Chapter 9.

Region   The Region tool allows you to configure your local regional settings as well as configure date and time formats.

RemoteApp And Desktop Connections   RemoteApp And Desktop Connections allows you to access programs and desktops on your network. To connect to these resources (remote applications and desktops), you must have the proper permission.

With RemoteApp And Desktop Connections, you can connect to either a remote computer or a virtual computer. To create a new connection, use the Set Up A New Connection Wizard included with the RemoteApp And Desktop Connections menu option.

Security And Maintenance   The Security And Maintenance utility has two configurable sections: Security and Maintenance. The Security section allows you to configure three different options:

- Spyware and unwanted software protection allows you to update Windows Defender.
- Virus protection allows you to install and configure virus protection.
- Windows Update allows you to update Windows 10.

The Maintenance section allows you to set up a Windows 10 Maintenance schedule. You can also set up a HomeGroup, file history, drive status, and device software in this section.

Sound   The Sound icon allows you to configure your machine's audio. You can configure output (speakers and audio drivers) and your input devices (microphones).

Speech Recognition   The Speech Recognition icon allows you to configure your speech properties. Speech Recognition allows you to speak into the computer and have that speech be displayed on the system. Many programs, including Microsoft Office, can display the words onscreen as you speak them into the system. You can complete the following actions via the Speech Recognition icon:

- Start Speech Recognition
- Set up a microphone
- Take speech tutorials
- Train your computer to better understand you
- Open the Speech Reference Card, which allows you to view and print a list of common commands

Storage Spaces   Storage Spaces in Windows 10 is another way to give your Windows 10 users data redundancy. Windows 10 administrators have the ability to group hard drives together into a storage pools. Windows 10 users can then use these storage pool capacities to turn the pools into individual Storage Spaces. You can configure your Storage Pools in this application.

Sync Center   The Sync Center allows you to configure synchronization between the Windows 10 machine and a network server. The Sync Center also allows you to see when synchronization occurred, if the synchronization was successful, and if there were any errors.

System   The System icon is one of the most important icons in Control Panel. The System icon allows you to view which operating system your machine is using, view installed system resources (processor, RAM), change the computer name/domain/workgroup, and activate Windows 10. From the System icon, you can also configure the following settings:

- Device Manager
- Remote Settings
- System Protection
- Advanced System Settings

Taskbar And Navigation   The Taskbar And Navigation icon allows you to configure how the taskbar, Start menu, and toolbars will operate.

Troubleshooting   The Troubleshooting icon in Control Panel allows you to troubleshoot common Windows 10 problems within the following categories:

- Programs
- Hardware And Sound
- Network And Internet
- System And Security

User Accounts   The User Accounts icon allows you to create and modify local user accounts. With the User Account icon, you can perform the following tasks:

- Change user passwords
- Remove passwords
- Change the account picture
- Change the account name
- Change the account type
- Manage user accounts
- Change user-account control settings

Windows Defender   Windows Defender is a built-in Windows 10 application that protects your system from spyware. It is included free with the operating system, and once you turn it on, it starts automatically protecting your system. Windows Defender can operate in different modes:

Real-Time Protection   In Real-Time Protection mode, Windows Defender runs in the background and protects your system as you are working live on the Internet or a network.

Scanning Option   When you're in Scanning Option mode, you can run a system scan at any time to check for spyware. This option does not require Windows Defender to always be running.

Command-Line Utility   Windows Defender includes a command-line utility called `MpCmdRun.exe`, which allows you to automate the use of Windows Defender. The `MpCmdRun.exe` utility is located in the `%ProgramFiles%\Windows Defender\` folder.

Windows Firewall   Windows Firewall helps prevent unauthorized users or hackers from accessing your Windows 10 machine from the Internet or the local network. Windows Firewall is explained in detail in Chapter 9.

Windows To Go   Windows To Go gives an administrator or user the ability to provision Windows 10 onto an external USB drive. You can then use the USB drive (known as a Windows To Go workspace) to load a complete and managed Windows 10 system image into a managed or unmanaged Windows 10 host computer to boot and run the Windows 10 operating system.

Work Folders   Work Folders allow a user to make data files available on all of the devices that he or she uses. You can access that data even when the devices are offline.

Now that we have taken a brief look at most of the icons in Control Panel, let's look at the System icon in greater detail.

Understanding the System Icon

The System icon (shown in Figure 5.22) in Control Panel is the gateway to a very useful set of utilities and tasks that can enable you to specify remote settings, device settings, system protection, and the computer name, among other things.

FIGURE 5.22   The System page
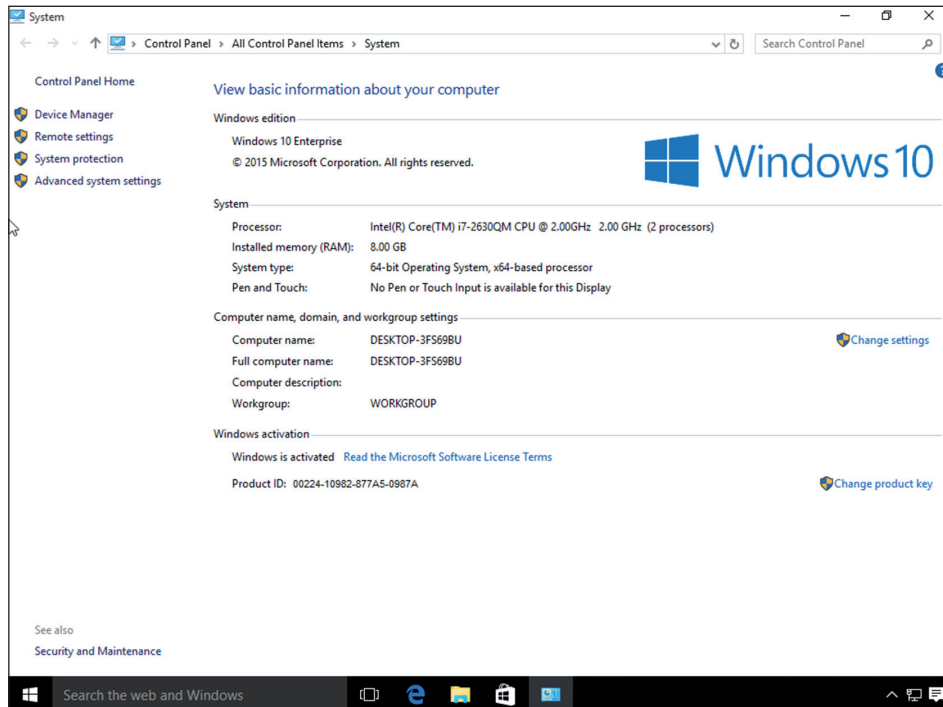
Let's look at the different utilities and tasks that can be configured in Control Panel:

Windows Edition   The Windows Edition section shows you which edition of Windows the machine currently has installed. The Windows Edition section also shows whether service packs are installed.

System   The System section shows the following information about the system hardware:

- Processor
- Installed memory (RAM)
- System type
- Pen and touch-screen availability

Computer Name, Domain, And Workgroup Settings   In the Computer Name, Domain, And Workgroup settings section, you can change the name of the computer system and also change the workgroup or domain. Windows 10 works well with Windows Server 2012 R2, which is explained in greater detail in Chapter 9.

Windows Activation   The Windows Activation section allows you to activate your Windows 10 operating system and change your product key before activating.

If you look to the left side of the System windows, you will see that there are four additional links: Device Manager, Remote Settings, System Protection, and Advanced System Settings. Let's take a look at some of these settings.

Device Manager   The Device Manager icon allows you to configure the different devices on your Windows 10 machine. You can configure such devices as disk drives, display adapters, DVD/CD-ROM drives, monitors, and network adapters.

Remote Settings   In the Remote section, you can set the Remote Assistance and Remote Desktop settings for the Windows 10 system. Windows Remote Assistance allows an administrator to connect to a machine and control the mouse and keyboard while the user is logged on with the administrator. This option can be enabled or disabled.

System Protection   The System Protection section is for configuring restore points and recoverability for the Windows 10 operating system. You can also manage disk space and all of your restore points from the System Protection section.

Advanced System Settings   The Advanced System Settings section allows you to set up such items as visual effects, processor scheduling, memory usage, virtual memory, desktop settings, system startup, and recoverability.

There are three main sections within the Advanced System Settings section:

Performance   The Performance section allows you to configure the visual effects, the virtual memory, processor scheduling, and Data Execution Prevention for the Windows 10 operating system.

The virtual memory is a section of the hard drive that is used by the system and RAM. Think of RAM as a pitcher of water. As the water fills up the pitcher, the pitcher becomes full. Once it's full, more water would cause it to overflow. The virtual memory

is the overflow for RAM. When RAM fills up, the oldest data in RAM gets put into the virtual memory. This way, the system does not need to look at an entire hard drive for that data. It finds it in the virtual memory.

The Data Execution Prevention section (found under the Settings button) helps protect against damage from viruses and other security threats.

User Profiles   The User Profiles section allows you to copy, delete, or move a user's desktop profile to another location or user account.

Startup And Recovery   The Startup And Recovery section allows you to configure which operating system will be booted by default (important for dual-booting machines) and what should happen when the system gets a startup error.

Let's now look at how to configure some of the options using the System icon. Complete Exercise 5.3 to change the computer name.

EXERCISE 5.3

Changing the Computer Name

1. Open the System tool by right-clicking Start ➢ Control Panel ➢ System.

2. Under the Computer Name, Domain, And Workgroup settings section, click the Change Settings link.

3. Click the Change button in the To Rename This Computer section.

4. In the Computer Name field, rename your computer. Click OK.

5. A dialog box asking you to reboot the machine will appear. Click the OK button.

6. Click the Close button, and then click the Restart Now button.

Now that you have renamed the computer, let's look at how to configure performance options. Complete Exercise 5.4 to manipulate your system's virtual memory.

EXERCISE 5.4

Changing the System's Virtual Memory

1. Open the System tool by right-clicking Start ➢ Control Panel ➢ System.

2. In the left side, click the Advanced System Settings link.

3. Under the Performance section, click the Settings button.

4. When the Performance option screen appears, click the Advanced tab.

5. In the Virtual Memory section, click the Change button.

6. Uncheck the Automatically Manage Paging File Size For All Drives check box.

7. Click the Custom Size radio button.

EXERCISE 5.4 *(continued)*

8. Set the Minimum and Maximum settings to two times the size of your RAM. For example, if your RAM is 4,096 MB, set the settings to 8,192 MB.

9. Click the Set button.

10. Click OK. Then click OK again at the Performance Options screen.

11. Close the System Properties screen.

> **NOTE**   Microsoft Windows 10 handles the virtual memory requirements by default, but I recommend increasing the virtual memory on your machine if hard drive space is available. I use the rule of thumb of one and a half to two times the size of RAM.

We have now talked about the Control Panel and the System icon, but we have not yet talked about the new Windows 10 Settings shortcut app. So in the next section, we are going to look at the Settings window.

Understanding the Settings Window

As stated earlier in the book, Windows 10 took the best of both Windows 7 and Windows 8 and created Windows 10. When you click the Start menu, you will see an option called Settings (see Figure 5.23).

FIGURE 5.23   The Settings option
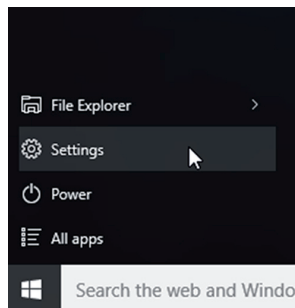
The Settings screen is a new way to configure different parts of the Windows 10 system. When you click the Settings option from the Start menu, you will see the Settings screen appear, as shown in Figure 5.24.

FIGURE 5.24   The Settings screen
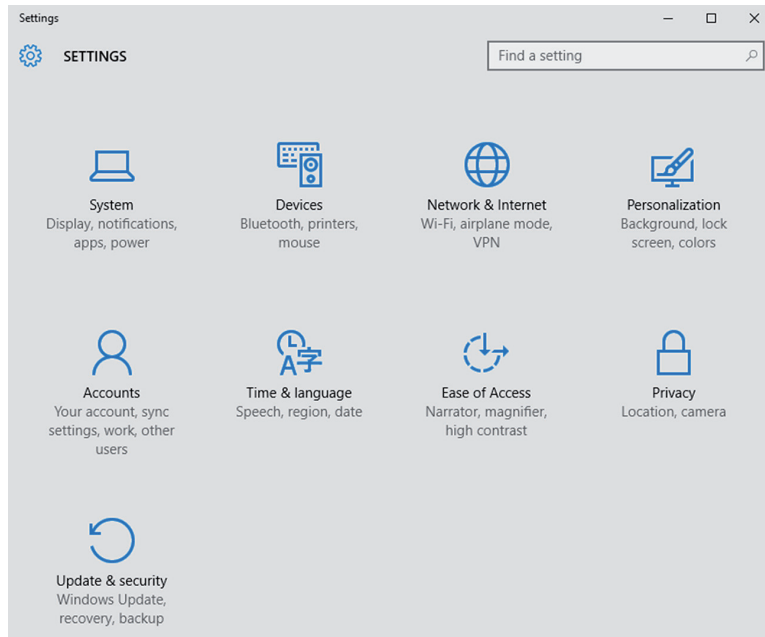
As you can see from Figure 5.24, the Settings Window has multiple sections of Windows 10 that you can configure. The following areas are settings that can be configured using the Settings screen:

- System
- Devices
- Network & Internet
- Personalization
- Accounts
- Time & Language
- Ease of Access
- Privacy
- Updates & Security

Most of these sections have already been covered previously in this chapter, and many of the other sections (such as Accounts) will be covered in other chapters of the book. I just wanted to make sure that you understand that it's another way to configure many of the same options that we have already looked at.

The one area that I would recommend that you look at right away is the choice for Privacy. Microsoft has turned many features on where Microsoft and other third-party vendors can access data on your system and also get information on how you use your Windows 10 system. Take a few minutes to look through the Privacy section and make sure that nothing is on by default that you don't want turned on.

Now that we have looked at how to do configurations for Windows 10, let's go ahead and take a look at how Windows 10 mobility works.

Understanding Mobility Options

So during this chapter we talked about all of the different icons in the Control Panel. Now we need to dive into a few of them in greater detail. The ones that we are going to discuss all have to deal with Windows 10 mobility.

Windows 10 is designed to be mobile and it has many features that revolve around that. Here are some of the mobility issues that we need to cover: how to configure offline file policies, configure power policies, configure Windows To Go, configure Wi-Fi direct, and configure sync options using the Sync Center.

Configuring Offline Files and Synchronization

One of the advantages of Windows 10 is how the operating system works and synchronizes with other systems and data.

The term *synchronization* could mean different things to different people. We could be talking about synchronization of offline files and data, or we can be talking about synchronization between two systems like a Windows 10 system and cloud-based Azure or OneNote.

In this section, we will talk about both. We will address synchronization between offline and online files, and we will discuss synchronization between Windows 10 and cloud-based services.

Offline Files allows network files to be available to clients even when a network connection to the server is unavailable or slow. When a user is accessing a server that is unavailable or when the network connection is slower than a configurable threshold, files are then retrieved from the Offline Files folders.

The Offline Files feature is enabled by default on the following client computer operating systems: Windows 10 Professional, Windows 10 Enterprise, and Windows Education. This feature is turned off by default on Windows Server operating systems.

Because in many organizations Windows 10 will be loaded onto a laptop computer, offline file access can be an important part of how Windows clients stay current even while off the network.

When you decide to turn synchronization on, Windows will automatically keep track of your synchronization choices for you on all of your Windows 10 devices (as long as you are

logged on to all of the Windows devices using the same account or have set up synchroniza-
tion with the other accounts and your Microsoft account).

Users have the ability to choose what items that they want to synchronize. For example,
users can synchronize passwords, web browser settings, File Explorer settings, and even
notifications.

To truly have synchronization work the way that Microsoft has intended, you need to
link all of your devices together using your Microsoft account or have your other accounts
linked to your Microsoft account. This includes your school or work accounts all tied into
one Microsoft account.

As an IT director for many years, I feel a bit uneasy about this idea. I truly believe that
linking your personal accounts together to synchronize all of your personal data is a good
way to go, but for obvious security reasons, I don't agree with corporate users linking into
their personal accounts.

So how do we go about synchronizing everything in Windows 10 easily? The best
method is to use the Sync Center in Control Panel (just right-click the Start ➢ Control
Panel ➢ Sync Center).

The Sync Center is built into Windows 10, and it's a one-stop shop for all of your
synchronization needs, including working with offline files (see Figure 5.25).

FIGURE 5.25   The Sync Center
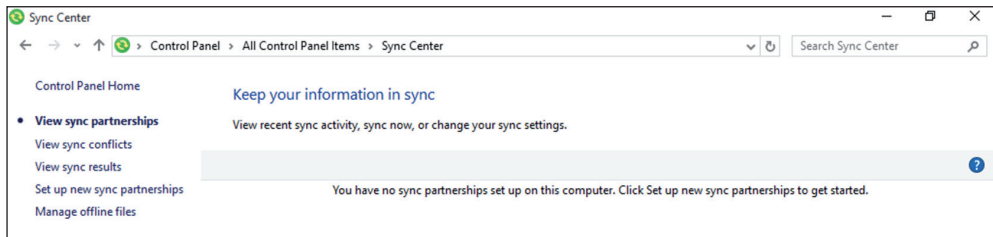
As you can see in Figure 5.25, you can set up synchronization between other devices
and partnerships. The figure shows you can also manage offline files. To manage offline
files, you have to enable that on the Windows 10 system (done through Sync Center) and
then also configure offline folder access with the Windows servers that you have at your
company.

When you click the link to Manage Offline Folders and enable offline folder access, you
then have three tabs that can help you set up offline folder access properly:

Disk Usage   The Disk Usage tab will show you how much disk space is currently being
reserved on the Windows 10 system for keeping offline files. You can change the amount of
space that is set for the Windows 10 system by clicking the Change Limits button.

Encryption   To make sure that the offline files are encrypted while on the system, click the Encryption button. The files will get encrypted based on your user's Security Identification (SID) number. When you log into the Windows 10 account using the account with the matching SID number, the files will become automatically decrypted when they are opened. If someone with a different user ID (SID) number tries to access these files, he or she will be denied access.

Network   The Network tab allows you to set a time interval (such as 5 minutes), and when that interval is hit, the Windows 10 system will automatically check the network connection to make sure that the connection is not on a slow connection. For example, when you are at home and you don't have direct access to your network, the Windows system will automatically revert to using the offline files due to the connection being slow or not available.

Configuring Power Policies

Earlier in the chapter, we started talking about the Windows 10 Power options. Power options allow a user or administrator to maximize their Windows 10 machine's performance and/or conserve energy.

Administrators or users have the ability to enter your own power restrictions to customize their machine. Power options are important settings when you are dealing with laptops. Since many laptops use batteries, power options allow you to get the most time from their batteries.

Now here is the kicker! Depending on what type of system you are on, you will see different options when you look at your power plan options. For example, Figure 5.26 shows the power plan options for a desktop system. You can tell that the only real options you have is what happens when you choose when to turn off the display or change your power consumption options.

FIGURE 5.26   Desktop power plan options
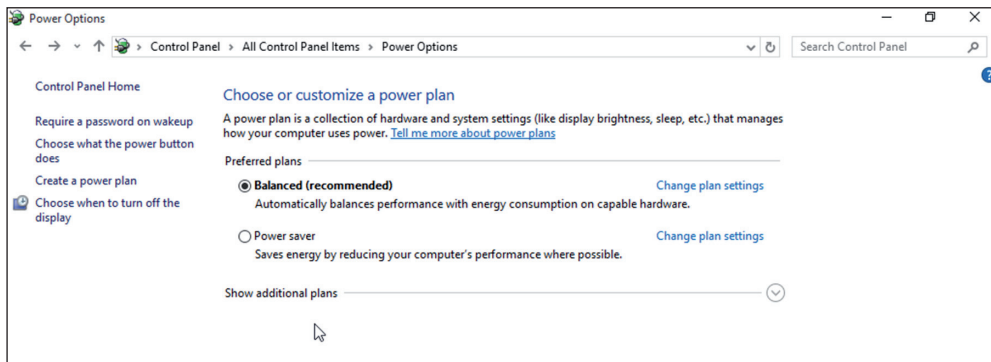
However, if you look at Figure 5.27, you can see that you have additional options based on whether your laptop or tablet is plugged in. You will not have those options on a desktop, because most desktops can't work when unplugged (unless you have a magical desktop).

FIGURE 5.27   Laptop power plan options
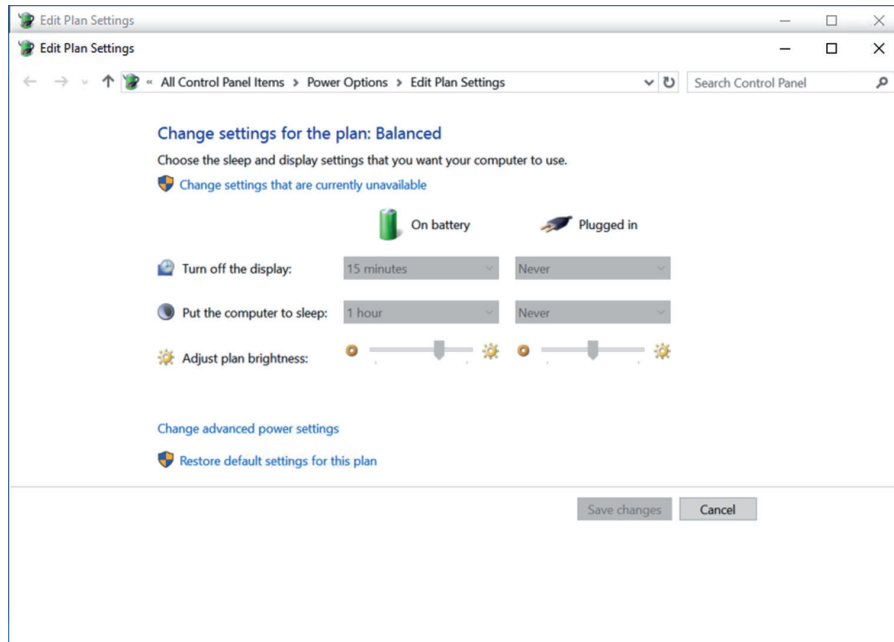
So setting up your power options really depends on what type of machine or tablet you're using. But some of the settings are the same no matter which one you use. The following are just some of the options that are the same no matter what type of Windows 10 system you're on:

- Require a password on wakeup
- Choose what the power button does
- Create a power plan

Laptops will have additional choices such as what happens when you close the lid of the laptop. No matter what type of system you are on, you can choose to go into advanced options and set very specific options on what system components would do while the system was running or while the system was idle.

For example, you can tell the system when the network card or hard drive can go into a sleep mode based on idle time (amount of time while no one is working on the system). So if you want to configure each individual component and how it should work while active or idle, you can go into the advanced options and configure each component separately.

Managing Power States

In Windows 10, 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 10 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 memory, and that session is available within seconds when the computer wakes. The computer can thus be put into a power-saving state when not in use but allows quick access to the in-process user session, so the user can 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 your desktop state as well as any open files to the hard drive. To use the computer again, you need to 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 onto 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 and 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.

The hibernation mode may not be available on your Windows 10 laptop machine by default. You must make sure your firmware can support hibernation before attempting to enable it. Now let's take a look at the different types of power options that you can configure.

Managing Power Options

You configure power options through the Power Options Properties dialog box. To access this dialog box, right-click Start ➢ Control Panel ➢ 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 10 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 10, 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 1 hour of idle time. You can modify these times as needed. Other power options that you can modify include Wireless Adapter settings and Multimedia settings. Wireless adapters can be configured for maximum power savings

or maximum performance. By default, the Balanced power plan configures wireless adapters for maximum performance. Additionally, you can configure the Multimedia settings so that the computer will not be put into sleep mode when sharing media. 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 1 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 new Allow The Computer To Enter Away Mode option. Away mode configures the computer to look like it's 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 5.1.

TABLE 5.1 Windows 10 power plans

Power Plan	Turn Off Display	Put Computer to Sleep	Turn Hard Disks Off
Balanced	After 20 minutes	1 hour	
Power Saver	After 20 minutes	1 hour	After 20 minutes
High Performance	After 20 minutes	Never	

In Exercise 5.5, I will show you how to configure a power plan for your computer.

EXERCISE 5.5

Configuring a Power Plan

1. Right-click Start ➢ Control Panel ➢ Power Options.

2. Select a power plan to modify from the Preferred Plans list, and click Change Plan Settings.

3. Configure the power-plan options for your computer based on your personal preferences. Click Change Advanced Power Settings to modify the advanced power settings. When all changes have been made, click Save Changes.

4. Close Control Panel.

Other desktop options you can use are the power button and switching users. Let's take a look at these features.

Configuring the Power Button

Unless you decide to run your computer 24 hours a day, you will eventually want to shut it down. By default, the Start menu has a power button. When you click this button, your machine will power off. But the power button does not have to be set to the Shut Down option. You can configure this button to Switch User, Logoff, Lock, Restart, or Shut Down.

You may have a machine that is shared by multiple users, and it may be better for you to have the Switch User button instead of the Shut Down button on the Start menu. Configuring the Switch User option would make it easier on your users.

In Exercise 5.6, you will configure the power button to the Switch User option.

EXERCISE 5.6

Configuring the Power Button to the Switch User Option

1. Right-click Start ➢ Control Panel ➢ Power Options.

2. On the left side, click Choose what the power button does.

3. From the Power Button Settings drop-down menu, choose Hibernate.

4. Click OK.

5. Click the power button and see if the system goes into the Hibernate mode. Once the system is brought out of the Hibernate mode, redo this exercise and choose Shut Down in step 3 to return the system to normal (if it was set to turn off).

After you decide how the power button is going to be used, you may want to config-ure some of the advanced power options. In the next section, we will look at the different power options.

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, right-click Start ➢ Control Panel ➢ Power Options and select the power plan to use. Then click Change Advanced Power Settings to open the Advanced Settings tab of the Power Options dialog box and 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 com-puter 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 hibernation mode.

Configuring Hibernation

Although sleep is the preferred power-saving mode in Windows 10, hibernation is still available for use. Hibernation for a computer means that anything stored in memory is written to 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 by loading the hibernation reserved area of hard disk back into memory. To configure your computer to hibernate, complete the same steps as you did previously in Exercise 5.6.

Command-Line Configuration

Microsoft gives you the ability to configure and manage your power settings through the use of the command line. The `Powercfg.exe` tool allows you to control power settings and configure computers to default to hibernate or standby mode. The `Powercfg.exe` tool is installed with Windows 10 by default. `Powercfg.exe` has a few switches that provide you better functionality. Table 5.2 describes some of these switches.

TABLE 5.2   `Powercfg.exe` switches

Switch	Description
`-change`	Changes a setting in the current power scheme.
`-changename`	Changes the name of a power scheme. Also gives you the ability to change the description.
`-delete`	Deletes the power scheme of the GUID specified.
`-deletesetting`	Deletes a power setting.
`-energy`	Looks for common energy-efficiency and battery-life issues and displays these issues in an HTML format. This switch is used to identify problems with the power scheme.
`-list`	Shows all the power schemes in the current user's environment.
`-query`	Shows the content of a power scheme.
`-qh`	Displays the content (including hidden content) of the power scheme.
`-waketimers`	Enumerates the wake timers. If this is enabled, when the wake timer expires, the system will wake from hibernation or sleep state.

> **NOTE**
>
> For a complete list of `Powercfg.exe` switches, visit the Microsoft website here:
>
> https://technet.microsoft.com/en-us/library/
> cc748940%28v=ws.10%29.aspx?f=255&MSPPError=-2147217396

There is a useful tool when you're using a laptop on the battery that allows you to see how much time you have left until the battery dies. Let's take a look at the battery meter.

Managing Power Consumption Using the Battery Meter

Windows 10 includes a battery meter that you can use to monitor the battery-power consumption on your mobile computer (laptop or tablet). The battery meter also provides notification as to 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 among the preferred power plans available with Windows 10.

Configuring Windows To Go

As stated earlier, Windows To Go gives an administrator or user the ability to provision Windows 10 onto an external USB drive. You can then use the USB drive (known as a Windows To Go workspace) to load a complete and managed Windows 10 system image into a managed or unmanaged Windows 10 host computer to boot and run the Windows 10 operating system.

Many of us carry a USB drive with us or maybe even on your key ring. Well, think about having a copy of Windows 10 with you wherever and whenever you want to use it. So what are the requirements to set up a Windows To Go drive? Well, you need a USB drive certified for Windows To Go use and an image of Windows 10 Enterprise. If you try to load a USB that isn't certified, you will receive the error, as shown in Figure 5.28.

FIGURE 5.28 USB non-compatible error
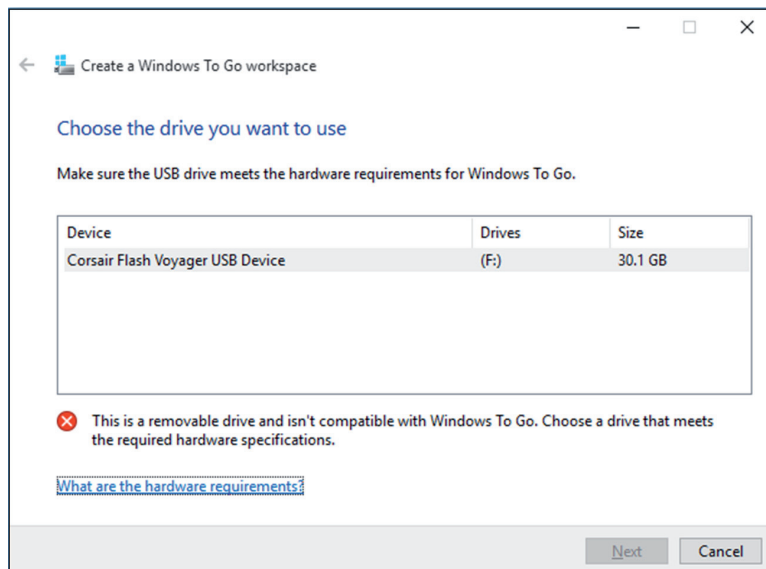
At the time that this book was written, the following list of USB drives are certified for Windows To Go:

- IronKey Workspace W700
- IronKey Workspace W500
- IronKey Workspace W300
- Kingston DataTraveler Workspace for Windows To Go
- Spyrus Portable Workplace
- Spyrus Secure Portable Workplace
- Spyrus Worksafe
- Super Talent Express RC4 for Windows To Go
- Super Talent Express RC8 for Windows To Go
- Western Digital My Passport Enterprise

The information in Table 5.3 was taken directly from the Microsoft website regarding what is needed on the host's computer to be able to accept Windows To Go.

TABLE 5.3   Windows To Go Host requirements

Item	Requirement
Boot Process	Capable of USB boot
Firmware	USB boot enabled (PCs certified for use with Windows 7 or later can be configured to boot directly from USB; check with the hardware manufacturer if you are unsure of the ability of your PC to boot from USB)
Processor architecture	Must support the image on the Windows To Go drive
External USB Hubs	Not supported; connect the Windows To Go drive directly to the host machine
Processor	1 Ghz or faster
RAM	2 GB or greater
Graphics	DirectX 9 graphics device with WDDM 1.2 or greater driver
USB port	USB 2.0 port or greater

To configure a Windows To Go USB drive, you need to complete the following steps:

1. Place a copy of a Windows 10 Enterprise image (`.iso` file) on the host computer you will use for image storage.

2. Open your Downloads folder on the host computer where you placed the `.iso` image, right-click the Windows image `.iso` file, and select MOUNT ISO. The `.iso` file will then appear as a disk drive on the host computer.

3. Right-click Start ➢ Control Panel.

4. In Control Panel, select Windows To Go.

5. Insert a compatible USB drive into a USB port on the host computer.

6. On the Choose the Drive You Want to Use page, all attached USB drives appear. Choose the compatible USB drive you want to use, and then click Next.

7. The mounted `.iso` file should now appear on the Choose a Windows 10 Image page. If for some reason you don't see the `.iso` file, select Add Search Location to choose the mounted `.iso` file. Select the file, and then click Next.

8. On the Set a BitLocker Password (Optional) page, select the Use BitLocker With My Windows To Go Workspace check box to protect the drive with BitLocker Drive Encryption.

9. Enter a BitLocker password, confirm it, and then click Next.

10. On the Ready to Create Your Windows to Go Workspace page, select Create to create the Windows To Go workspace.

11. Choose a boot (startup) option, and then select Yes to modify the Windows Boot Manager configuration to boot automatically from your Windows To Go workspace when the drive is connected to this host computer.

12. When provisioning is complete, select Save And Restart to restart the host computer.

Configuring Wi-Fi Direct

To understand Wi-Fi Direct, you must first understand a bit about Wi-Fi and how it's used to connect to a network. So let's think about most of our home networks. You go to a big-box store to buy (or maybe order online) a wireless access point (WAP) such as Netgear or Linksys. Most of us have these at home connected to our Internet provider.

So we buy a wireless access point (WAP) like Netgear or Linksys and connect it to our Internet provider. We then connect our home systems to the wireless access points and BOOM, we all have Internet access.

Now think about being able to connect to devices without the use of a WAP. What if we could connect devices directly to each other through the high-speed wireless adapters in those devices? That is exactly what Wi-Fi Direct enables us to do.

Wi-Fi Direct is a technology that allows us to directly access other devices without requiring a separate Wi-Fi access point. Windows 10 uses near-field communication (better known as NFC) technology to allow the Windows 10 system to locate other NFC Wi-Fi enabled devices so that they can be paired together.

When devices are trying to pair together, the Near Field Proximity (NFP) receives pairing information from the device that is trying to connect. NFP then passes the pairing

information to Windows 10. Windows 10 Wi-Fi Direct will then automatically follow the Wi-Fi Alliance Out-Of-Box pairing procedures for the connection.

If the pairing process connects, Windows will prompt the user for permission for the connection. If permission is given, Windows 10 will then attempt to finalize the connection. From that point on, there is no other user interaction needed.

Windows 10 gives you the ability to set whether you want to pair with other devices or not. Figure 5.29 shows the Windows 10 Privacy settings and how Windows 10 will sync with other devices.

FIGURE 5.29 Sync with devices
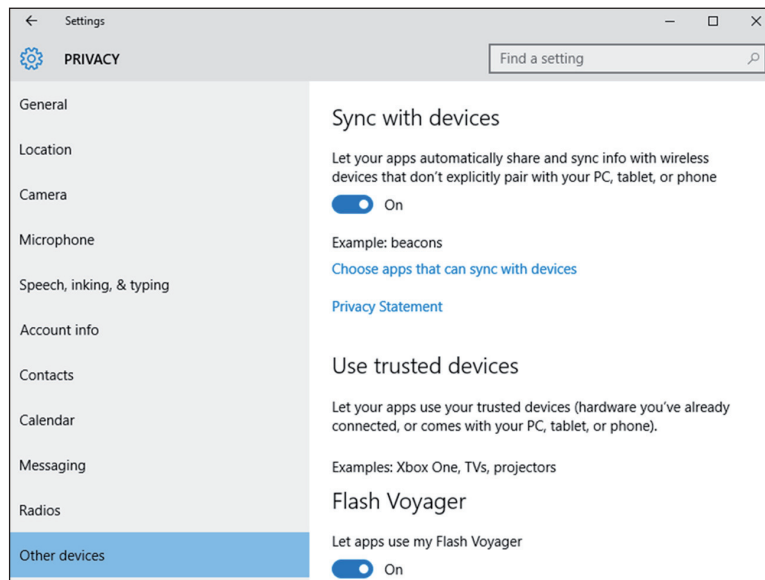
As you can see in Figure 5.29, you also have the ability to choose which applications can sync with devices. This gives an administrator or user better flexibility on whether to allow all applications to connect to all devices or only specific applications to connect.

Now that we have looked at how to use applications to configure the Windows 10 system, let's look at how we can configure the Windows 10 system by using the Registry.

Using the Registry Editor

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, which was discussed in the previous section.

WARNING 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 10 uses the REGEDIT or REGEDT32 program as the primary utility for Registry editing in Windows 10. It does not matter which program you use; both support full editing of the Registry. To use REGEDIT, select Start and type **REGEDIT** in the Search dialog box. To use REGEDT32, type **REGEDT32** into the Search dialog box.

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 described in Table 5.4.

TABLE 5.4 Registry keys

Registry Key	Description
HKEY_CLASSES_ROOT	Configuration information used by Windows Explorer to properly associate file types with applications.
HKEY_CURRENT_USER	Configuration information for the user who is currently logged onto the computer. This key is a subkey of the HKEY_USERS key.
HKEY_LOCAL_MACHINE	Computer hardware configuration information. This computer configuration is used regardless of the user who is logged in.
HKEY_USERS	Configuration information for all users of the computer.
HKEY_CURRENT_CONFIG	Configuration of the hardware profile that is used during system startup.

Earlier in this chapter, I showed you that Remote Desktop Connection is one of the configurable Windows 10 options. In the next section, we will look at configuring different ways to remotely connect using the Windows 10 operating system and how to allow others to remotely connect to you for assistance.

Configuring Remote Connections

End-user support is a major concern and a time-consuming endeavor for most IT departments. Anything you can do to provide a more efficient solution to user issues is a major benefit. Basic telephone or chat support works in many cases, but what if you could see what the end user sees or even interface with their machine? By using Remote Assistance and Remote Desktop, you can.

Remote Assistance in Windows provides many enhancements over previous versions, including improvements in security, performance, and usability. Windows 10 goes even further by adding Easy Connect, which makes it easier for novice users to request help from expert users. Group Policy support has been increased. There is command-line functionality (meaning you can add scripting), bandwidth optimization, logging, and more.

Remote Desktop is a tool that allows you to take control of a remote computer's keyboard, video, and mouse. This tool does not require someone collaborating with you on the remote computer. Remote Desktop is used to access remote machines' applications and troubleshoot issues as well as meet end-user needs where you want complete control of the remote machine.

We'll start the discussion with Remote Assistance. Later in this section, we will also look at how to use virtual private networks (VPNs). We will look at how to configure VPNs and the protocols that work with VPNs.

Remote Assistance

Remote Assistance provides a method for inviting help by instant message, email, a file, or now an Easy Connect option. To use Remote Assistance, the computer requesting help and the computer providing help must have Remote Assistance capabilities and the feature enabled, and both computers must have network connectivity (they have to be able to talk to each other).

Remote Assistance is designed to have an expert user (the assistor) provide assistance to a novice user (assistee). When assisting a novice user, the expert can use text-based chat built into Remote Assistance. The expert can also take control of a novice user's desktop (with permission, of course). Here are two common examples of when you would use Remote Assistance:

- Diagnosing problems that are difficult to explain or reproduce. Remote Assistance can allow an expert to remotely view the computer, and the novice user can show the expert an error or problem.

- Guiding a novice user to perform a complex set of actions. The expert can also take control of the computer and complete the tasks if necessary.

Easy Connect

The Easy Connect method for getting remote assistance is new for Windows 10. Easy Connect uses Peer Name Resolution Protocol (PNRP) to set up direct peer-to-peer transfer using a central machine on the Internet to establish the connection. PNRP uses IPv6 and Teredo tunneling to register a machine as globally unique. You're not using IPv6? You are with PNRP; Windows 10 (as well as Windows 7/8, Windows Server 2008/2008 R2, and Windows Server 2012/2012 R2) has IPv6 turned on natively as well as the currently used standard of IPv4. We'll discuss IPv6 in more detail in a later chapter, but to give you an idea, you can see the structure of the PNRP Teredo IPv6 packet in Figure 5.30.

To establish a Remote Assistance session with a user using Easy Connect, the novice should open the Windows Remote Assistance screen by right-clicking Start ➢ System ➢ Remote Settings ➢ Remote tab. You can also launch the Windows Remote Assistance screen by typing **msra** in the integrated search box next to the Start menu.

FIGURE 5.30 Teredo and IPv6 PNRP structure

Remote Assistance can also be incorporated in Group Policy in an enterprise environment by having the expert user configured as a Helper for users in the enterprise (by domain or OU). Once configured as a Helper, the expert can initiate a Remote Assistance session by issuing the command msra /offerra. This will bring up the Who Do You Want To Help Remote Assistance screen.

The expert can also include the novice user's IP address or computer name as an option to the offerRA switch to initiate the Remote Assistance session in one stop (e.g., msra / offerra *ipaddress | computername*).

There are several msra.exe switches available to further control the establishment of the Remote Assistance session for both the novice and the expert user. Table 5.5 highlights many of the switches.

TABLE 5.5 MSRA command-line switches

Switch	OS Availability	Functionality
/?	Vista and above	Displays the help options.
/novice	Vista and above	Starts Remote Assistance at the Invite screen.
/expert	Vista and above	Starts Remote Assistance at the Help Someone screen.
/offerRA *ip | computer*	Vista and above	Starts Remote Assistance at the Expert Initiated screen or with the options, by automatically initiating with the novice user (used with Group Policy configured in an enterprise environment).
/email *password*	Vista and above	Creates an email invitation to be sent to an expert user to request assistance using the novice's default email program; a random password will be generated and needs to be conveyed to the expert, or alternatively a password can be specified with the password option and conveyed to the expert.

Switch	OS Availability	Functionality
`/saveasfile` *path* *password*	Vista and above	Creates a file invitation to be given to an expert user to request assistance; a random password will be generated, or optionally a password can be specified with the *password* option and conveyed to the expert.
`/openfile` *path*	Vista and above	Used to open the invitation file sent to the expert; can be local or on a shared network drive; the expert will enter the password given to the user when the session was initiated.
`/geteasyhelp`	Windows 7 and above	Starts a novice user's Remote Assistance session using Easy Connect; presents the novice with the password to convey to the expert user.
`/offereasyhelp`	Windows 7 and above	Starts an expert user's Remote Assistance session using Easy Connect; presents the expert user with the screen to enter the password from the novice user.
`/getcontacthelp` *address*	Windows 7 and above	Reestablishes a Remote Assistance session from a novice user's machine to the address from the previous session. The address is in the `RAContactHistory.xml` file as a 20-byte hexadecimal string with an `.RAContact` extension.
`/offercontacthelp` *address*	Windows 7 and above	Reestablishes a Remote Assistance session from an expert user's machine to the address from the previous session. The address is in the `RAContactHistory.xml` file as a 20-byte hexadecimal string with an `.RAContact` extension.

Whichever way the novice or the expert launches the feature, the Windows Remote Assistance screen will become available (see Figure 5.31). To start using Easy Connect, the novice user will select Invite Someone You Trust To Help You.

One nice feature of Easy Connect is that if the novice user has established an Easy Connect session previously with an expert user, the screen after selecting Use Easy Connect will offer the novice the ability to connect to the same expert. The novice user can also choose to invite someone new and/or delete the old contact. The expert user will have the same option after choosing Use Easy Connect from the machine used for a previous Easy Connect session.

After the Use Easy Connect option is selected, Windows 10 will verify network connectivity briefly. This is the point at which the PNRP actions take place and the novice user's information is added to a cloud on the Internet. The cloud is the group of machines holding little pieces of information—the identifiers of users needing connectivity, set up in

a peer-to-peer sharing environment. PNRP uses this distributed infrastructure for its peer-to-peer name resolution. The novice user's contact information is entered into the PNRP cloud, and an associated password is created and displayed to the novice user.

FIGURE 5.31 Remote Assistance initial screen
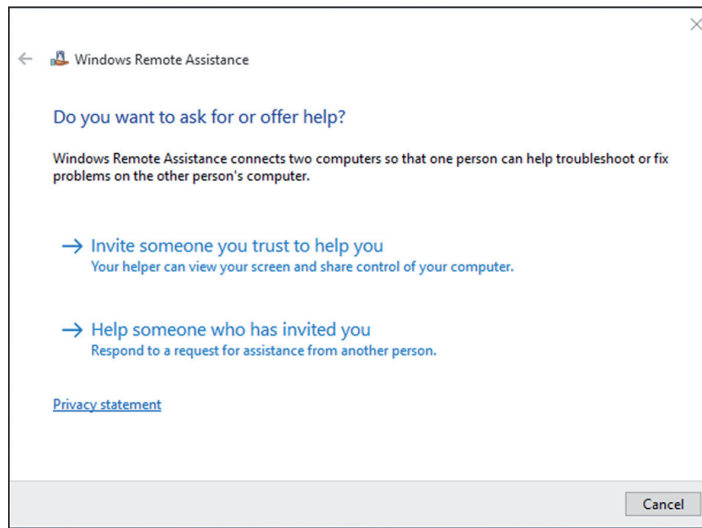
The novice user will now relay the password to the expert by text message, telephone, or any convenient conversation method. The novice will simply have to wait for the expert to initiate their part. The novice user will still have to accept the connection once the expert starts the remote assistance session.

The expert user needs to start a Remote Assistance session the same way the novice did in Figure 5.31, but the expert will choose "Help Someone Who Has Invited You" from the Windows Remote Assistance screen.

The expert user will be presented a dialog box to "use an invitation file" (Figure 5.32) and then, after choosing the file, will be prompted to enter the password to connect to the Remote Assistance session.

After a few moments of querying the PNRP cloud and finding the connection information that provides the path back to the novice user, Remote Assistance presents the novice user a confirmation box verifying that the user wants to allow help from the expert.

The novice user will then have a control bar on their screen indicating that the Remote Assistance session is active. From this control bar, the novice can initiate a chat session with the expert and modify some general session settings (bandwidth, logging, contact information exchange, and sharing control).

The expert user will be shown the novice user's desktop within a separate Remote Assistance window. The expert user will also have some general configuration-setting capabilities as well as an option to request control of the novice user's desktop. The novice user will, of course, be allowed to accept or reject the expert's request.

FIGURE 5.32   Remote Assistance screen for entering a password
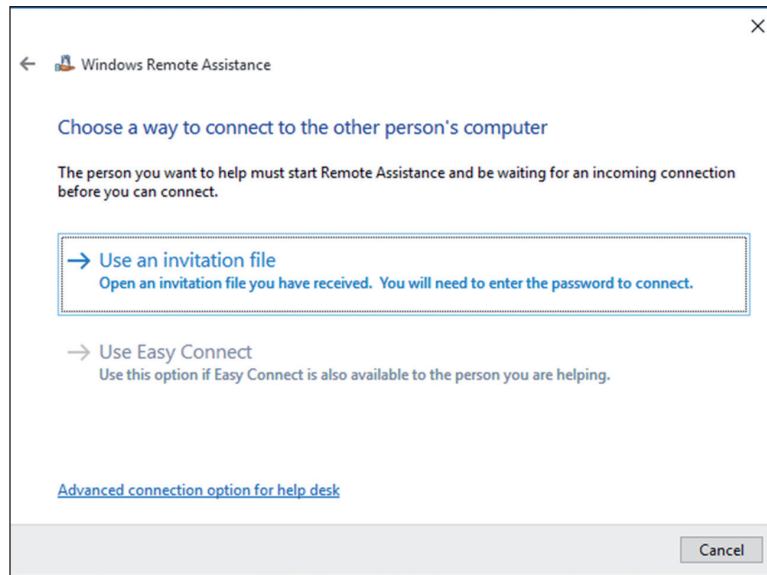
The expert and novice user can now have an interactive session in which the necessary assistance can be provided. This method of help really takes out the "can you tell me what you see on your screen" issues between two users. The Easy Connect feature takes one more problem out of the equation, getting a novice user to send an invitation to another user. The one caveat here is that both users must be using Windows 10 for Easy Connect to be an option.

Now what if the user is not available to send you the invitation? You can still connect to a user's computer using Remote Desktop, which I will discuss in the next section.

Remote Desktop

Remote Desktop is a tool in Windows 10 that allows you to take control of a remote computer's keyboard, video, and mouse. This tool does not require someone to be available to collaborate with you on the remote computer. While the remote computer is being accessed, locally it remains locked and any actions that are performed remotely will not be visible to the monitor that is attached to the remote computer.

Windows 10 Remote Desktop is, again, an enhanced version of the remote desktop functionality that has been with us for many of the previous versions of Windows, both client and server operating systems. Remote Desktop uses Remote Desktop Protocol (RDP) to provide the data between a host and a client machine. Windows 10 Remote Desktop features are as follows:

- RDP Core Performance Enhancements
- True Multi-Monitor Support

- Direct 2D and Direct 3D 10.1 Application Support
- Bi-directional Audio Support
- Multimedia and Media Foundation Support
- Remote FX has a few end-user enhancements for RDP. These enhancements allow for an enhanced desktop environment within your corporate network.

There are many uses for Remote Desktop, but the most common use is that of the administrator attempting to perform a task on an end user's machine (or on a server).

Another use is the end user connecting to a machine from their home or on the road. If you have noticed the enhancements of Remote Desktop (which are enhancements to RDP), you can see that one of the main goals of enhancing Remote Desktop is to make the user experience as comfortable and seamless as possible.

🌐 Real World Scenario

Using Remote Desktop Functionality

As an administrator, I like to just take control of an end-user machine and fix it. Although this can be done in Remote Assistance, the end user is required to allow us to have access and then can watch what I do. In Remote Desktop, I just take control and close the interactive session at the remote machine (yes, the remote end user can block us or take over the session, but not if they want their problem solved).

But there are other uses as well. I provide servers with resources to our clients, and that server may need to be changed or updated on a regular basis (sometimes a couple of changes in a day). Remote Desktop allows me to maintain our servers from wherever we are without impacting the clients or other administrators.

Remote Desktop Connection Options

When connecting to a Remote Desktop host machine, several options are available to enhance the client user session. The options allow configuration for general settings, display options, local resource access, programs to be executed on startup, the user experience, and advanced options for security and Remote Desktop gateway access. The options become available by clicking the Options button in the lower-left area of the initial Remote Desktop Connection screen. Figure 5.33 shows the options window displayed.

From the General tab, you can select the target remote computer and username. You can save the user credentials from this tab as well. You can save the connection settings to a file or open an existing RDP file from the General tab.

From the Display tab you can choose the size of the display screen. This is also where you select the option to use multiple monitors. The color depth (color quality) is also selected in the Display tab. The option to display the connection bar when using full-screen display is available here as well.

FIGURE 5.33 Remote Desktop options
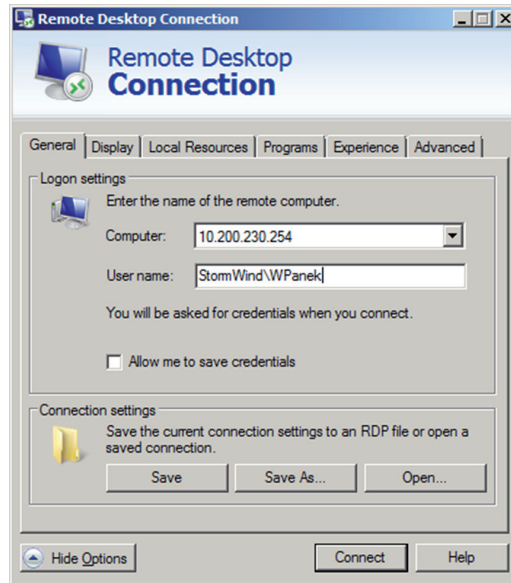
From the Local Resources tab you can configure remote audio settings, keyboard settings, and local device and resource access.

The Programs tab for Remote Desktop options allows the selection of a program to run at connection startup. The program name and path are specified, as is a startup folder if necessary.

The end-user experience is important to the overall success of using Remote Desktop in the user environment. Remote Desktop can be used to provide a user with the ability to connect to their machine and "remote in." The most seamless environment from the user to the remote location is desirable, but that will be dependent on the bandwidth available. The more bandwidth, the more high-end features can be made available to the end user.

This is also nice for the administrator who is working on an end-user machine. The Experience tab allows the configuration of the end-user experience.

Controlling the behavior of the Remote Desktop connection with regard to security is configured on the Advanced tab of the Remote Desktop options dialog box. The Advanced tab also supports the configuration of a Remote Desktop gateway to allow Remote Desktop connections to be established from any Internet location through SSL. The user must still be authorized, and the Remote Desktop client must still be available.

One very cool feature of using RDP is that if you connect from a touch-compatible device, your RDP session will have touch, regardless if the target machine has a touch screen. For example, if you are on a surface Pro and you RDP into a Windows 10 desktop without a touch-capable monitor, you will be able to control the Windows 10 desktop with touch options of the Surface Pro.

In Exercise 5.7, you will enable the Windows 10 machine to allow Remote Desktop connections. It is up to the company to decide whether all user machines are to be configured this way when you install Windows 10 or whether you should do this only when it becomes necessary for a given computer.

EXERCISE 5.7

Enabling Remote Desktop

1. Open the System tool by right-clicking Start ≻ Control Panel ≻ System.

2. On the left-hand side, click the Remote Settings link.

3. In the Remote Desktop section, click the radio button that allows connections from computers running any version of Remote Desktop (Less Secure).

4. Make sure the Allow Remote Assistance Connections To This Computer check box is checked.

5. Click OK.

6. Close the System Properties screen.

One way a Windows 10 user can connect to a server is through the use of a virtual private network connection. In the next section, we will look at how to configure a VPN connection on Windows 10.

Configuring a VPN Connection

A virtual private network is a way to establish a connection between a client machine (VPN client) and server machine (VPN server). A VPN gives you the ability to connect (called *tunneling*) to a server through the use of the Internet or a dial-up connection (hopefully not dial-up), typically with the intention of accessing resources that are available on the network where the VPN server is connected. The VPN server acts as a bridge for the external user connecting from the Internet or other external connections point, to the internal network. In a nutshell, a VPN allows you to connect to a private network from a public network.

VPN connections can be secured using various protocols. The following list shows you some of the tunneling protocols that can be used when connecting a Windows 10 machine to a remote server:

Internet Key Exchange version 2 (IKEv2)   Windows 10 can connect to a Windows Server VPN using the *Internet Key Exchange version 2 (IKEv2)* VPN tunneling protocol. The IKEv2 VPN protocol is the newest VPN protocol out of all of the following protocols and can be used with Windows Server 2012/2012 R2. The main advantage of using the IKEv2 VPN protocol is that it allows for the interruptions of the network connection. IKEv2 will

then automatically restore the VPN connection after the network connection is restored. This feature is referred to as VPN Reconnect, and it is automatically built into the IKEv2 protocol.

Secure Socket Tunneling Protocol *Secure Socket Tunneling Protocol (SSTP)* was released with Windows Server 2008 and is one of the tunneling protocols available with a Windows Server 2008/2008 R2 server and Windows 7 machines and later. SSTP works by allowing encapsulated Point-to-Point Protocol (PPP) packets to be transmitted over an HTTPS connection. Because of this, firewalls or Network Address Translation (NAT) devices allow SSTP VPN connections to be more easily established. SSTP is the best choice for securing a VPN connection.

Point-to-Point Tunneling Protocol *Point-to-Point Tunneling Protocol (PPTP)* is one of the predecessors to SSTP, and it also allows point-to-point packets to have encryption for secure connections. PPTP uses TCP/IP for the encryption. PPTP encapsulates PPP frames in IP and uses the TCP for the management side of PPTP.

Layer 2 Tunneling Protocol *Layer 2 Tunneling Protocol (L2TP)* is a tunneling protocol that has no encryption included in the protocol. L2TP uses the IP Security protocol (IPSec) to make L2TP secure. L2TP with IPSec is a much more secure tunneling option than PPTP.

   To set up an outbound client VPN connection in Windows 10, you use the Network And Sharing Center. In Exercise 5.8, you will set up a new VPN connection.

EXERCISE 5.8

Setting Up a VPN Connection

1. Start the Network And Sharing Center by right-clicking Start ➢ Control Panel ➢ Network And Sharing Center.

2. Choose the Set Up A New Connection Or Network link.

3. Choose Connect To A Workplace. Click Next.

4. Choose the Use My Internet Connection (VPN) option.

5. The Connect To A Workplace screen appears. You need to type in the TCP/IP address of a VPN Server and name this VPN connection. In this window, you also have the ability to use a smart card, to allow other people to use this connection, and to set up the VPN but not connect at this time (the option I chose). After you type in a TCP/IP address and name the VPN connection, click Next.

6. The next screen asks you for your logon credentials. Type in your username, password, and domain name. Click Create.

   Now that the connection is created, I'll show you the steps needed to use it.

7. In the lower-right corner, click your network connection.

8. A box appears showing your connections. To connect to the VPN connection, choose the corresponding link.

9. When the Connect dialog box appears, make sure your username, password, and domain name are present and click the Connect button.

10. After the connection is established, close it and close the Network and Sharing Center.

Transparent Caching

Windows 10 has a feature called *transparent caching* to help reduce the time needed for retrieving shared files and folders. Transparent caching reduces the time required to access files for the second and subsequent times across a slow network.

In previous versions of Windows, to access a file across a slower network, client computers had to retrieve the file from the server computer. But now with Windows 10 transparent caching, computers can cache these remote files, thus reducing the number of times a computer might retrieve the same data.

When a user opens a file for the first time, Windows 10 accesses the file from the server and then stores the file in the cache of the local disk. From that point on, the user reads the same cached file instead of reading it from the server computer.

To make sure the file is accurate; the Windows 10 client always contacts the server to ensure the cached copy is up to date. The file would not be accessible if the server is unavailable. Transparent caching is not enabled by default on fast networks. Transparent caching can be enabled through the use of a group policy.

Broadband Tethering

One nice advantage to Windows 10 and mobility is Broadband Tethering. Let's all pretend that we are at a large Microsoft conference and only one of us in our group can get onto the Internet. Windows 10 Broadband Tethering allows at least 10 devices to connect to your Internet connection and use your Internet for their access. As long as their devices have Broadband-enabled capabilities, they will be able to connect to your system and use the Internet.

When you set up the Broadband Tethering, you can set up a connection name and password for all of the other users in your group to connect to your system.

All you need to do is go to your Windows 10 mobile device (in Figure 5.34), I'm using a Windows 10 Surface Pro, and you just need to open your Internet connection by sharing the connection.

As you can see in Figure 5.35, once you open the connection up, you need to set up a password (at least eight characters), and then you can share that password with the other members of your group who you want to allow your Internet to be shared with.

In the next section, we will look at how to configure Windows 10 Services.

FIGURE 5.34   Manage Wi-Fi Settings
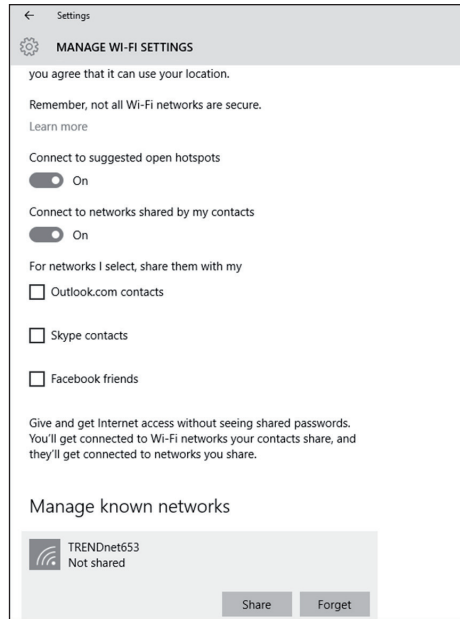
FIGURE 5.35   Manage Wi-Fi Settings password
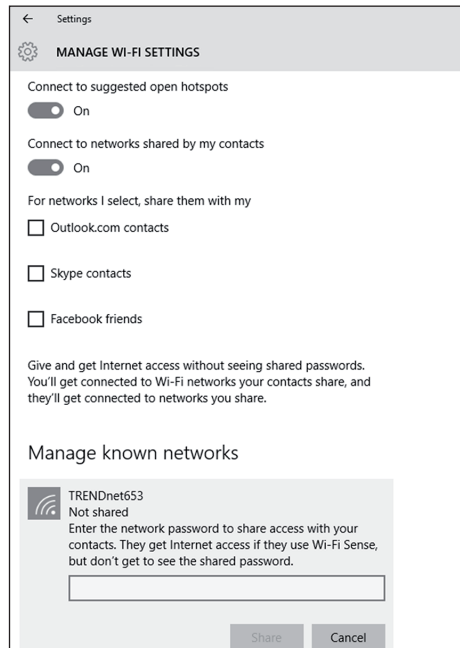
Managing Windows 10 Services

A *service* is a program, routine, or process that performs a specific function within the Windows 10 operating system. You can manage services through the Services window, which can be accessed in a variety of ways. If you go through the Computer Management utility, you can just right-click Start ➤ Computer Management ➤ Services And Applications. You can also go through Administrative Tools in Control Panel.

The Services window lists the name of each service, a short description, the status, the startup type, and the logon account that is used to start it. To configure the properties of a service, double-click it to open its Properties dialog box, shown in Figure 5.36. This dialog box contains four tabs of options for services: General, Log On, Recovery, and Dependencies.

FIGURE 5.36   The Properties dialog box for a service
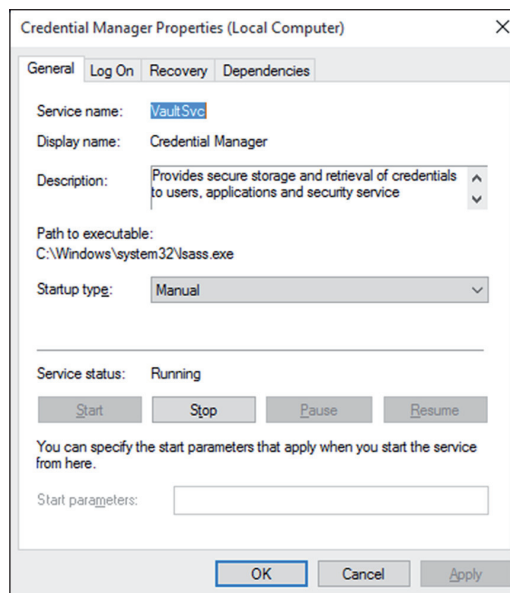
General   This tab allows you to view and configure the following options:

- The service display name
- The 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 state to start, stop, pause, or if paused you can also resume the service.

Log On The Log On tab 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.

Recovery The Recovery tab 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 a discrete action from the following list:

- 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. You can also specify how long until a machine is restarted if an error occurs.

Dependencies The Dependencies tab 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.

In Exercise 5.9, you will complete the steps needed to configure services in the Windows 10 operating system.

EXERCISE 5.9

Configuring Services

1. Start Computer Management by right-clicking Start ➤ Computer Management ➤ Services And Applications.

2. Click the Services link.

3. Scroll down the list and double-click Remote Desktop Configuration.

4. Under Startup Type, choose Automatic.

5. Under the Logon tab, click the This Account radio button.

6. Click the Browse button and choose the local administrator account. Click OK.

7. In the Password boxes, type and verify the administrator password.

EXERCISE 5.9 *(continued)*

8. In the Recovery tab, make sure the following settings are configured:

   Action: Response
   First Failure: Restart The Service
   Second Failure: Restart The Service
   Subsequent Failures: Take No Action
   Reset Fail Count After: 1 Day
   Restart Service After: 10 Minutes

9. Click the OK button.

10. Close the Computer Management MMC.

Services are just another troubleshooting and configuring tool that is part of your arsenal of troubleshooting techniques. Just remember that when your services are working properly, your Windows 10 operating system will be working properly.

Summary

Besides actually installing Windows 10, configuring the operating system properly is one of the most important tasks that an IT team can perform.

Configuring the desktop environment allows an administrator to configure an environment that is comfortable for the end user, which in turn makes the user more productive.

Understanding the Start menu and Control Panel icons allows you to configure and operate the Windows 10 applications more efficiently. Knowing how to configure the System icon properly in Control Panel allows you to fine-tune the Windows 10 operating system and get the best performance possible out of it.

In addition to using Control Panel to configure the Windows 10 operating system, you can edit the Registry directly using the REGEDIT or REGEDT32 utility.

Another important consideration when configuring Windows 10 is how the operating system will function when installed on a laptop or tablet (Windows Mobility). By configuring the mobility options on a laptop, you can allow that laptop to connect to their data in multiple ways.

We also looked at services that run on Windows 10 and how to configure and troubleshoot them when they don't run properly.

Video Resources

There are videos available for the following exercises:

>   5.1
>
>   5.2
>
>   5.3

  You can access the videos at `www.wiley.com/go/sybextestprep` on the Other Study Tools tab.

Exam Essentials

Be able to configure Desktop settings.   Understand how to customize and configure the Windows 10 Desktop settings. This includes setting a desktop and also setting up desktop personalization. It is also important to know how to configure the Taskbar and Start menu.

Be able to support mobile computers through power-management features.   Understand the new power features that are available in Windows 10 and be able to configure a laptop computer to use them.

Understand remote connections.   Know how to configure and connect to machines through remote connections. You can use Remote Assistance, Remote Desktop, and a VPN.

Know how to configure services.   Understand how to stop, start, monitor, pause, and configure services on the Windows 10 operating system. Know how to configure the different properties available through services.

Review Questions

1. You are the system administrator for your company. You are configuring the services on a Windows 10 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 your network wants to edit the Registry, including setting security on the Registry keys. What primary utilities that support full editing of the Windows 10 Registry should the system administrator use? (Choose all that apply.)

   A. REGEDIT

   B. REDIT

   C. REGEDT32

   D. REGEDITOR

3. Kayla 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

4. Denise 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

5. 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 the application is updated, 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`

6. You have a user, Rob, who uses a laptop computer running Windows 10. You have config-
ured the laptop to enter sleep mode after 30 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 memory, and the computer will be put into a power-saving
state.

7. You want to speed up the resume time on your computer after it is put into hibernation
mode. You have installed a hybrid hard-disk drive into your Windows 10 computer. Which
technology should you use to accomplish your goal?

 A. ReadyDrive

 B. ReadyBoost

 C. Superfetch

 D. SuperDrive

8. A new employee named Crystal has been supplied with a Windows 10 laptop computer.
You have configured Crystal's computer with the Power Saver power plan, and you used
the default options. Which of the following will occur after 20 minutes of inactivity on
Crystal'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.

9. You are the network administrator for a medium-size company. You support all user Desk-
top issues. Gary is using the default Windows 10 Desktop on his laptop computer. Gary
wants to change his Desktop settings. Which of the following options should Gary use to
configure the Desktop in Windows 10?

 A. Right-click an empty space on the Desktop and choose Personalize from the con-
text menu.

 B. Select Control Panel ➢ System.

 C. Right-click My Computer and choose Manage from the context menu.

 D. Right-click My Computer and choose Properties from the context menu.

10. 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.

Chapter

6

Planning and Managing Microsoft Intune

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Manage devices with Microsoft Intune.**

- This objective may include but is not limited to the following subobjectives: Provision user accounts, enroll devices, view and manage all managed devices, configure the Microsoft Intune subscriptions, configure the Microsoft Intune connector site system role, manage user and computer groups, configure monitoring and alerts, manage policies, manage remote computers.

✓ **Deploy software updates by using Microsoft Intune.**

- This objective may include but is not limited to the following subobjectives: Use reports and In-Console Monitoring to identify required updates, approve or decline updates, configure automatic approval settings, configure deadlines for update installations, deploy third-party updates.

✓ **Support mobile devices.**

- This objective may include but is not limited to the following subobjectives: Support mobile device policies including security policies, remote access, and remote wipe; support mobile access and data synchronization including Work Folders and Sync Center; support broadband connectivity including broadband tethering and metered networks; support Mobile Device Management by using Microsoft Intune, including Windows Phone, iOS, and Android.

✓ **Support Windows Store and cloud apps.**

- This objective may include but is not limited to the following subobjectives: Deeplink apps by using Microsoft Intune; sideload apps by using Microsoft Intune.

✓ **Support desktop apps.**

- This objective may include but is not limited to the following subobjective: Deploy desktop apps by using Microsoft Intune.

In this chapter, we will start diving into the world of the cloud. I am going to talk about Microsoft Intune and how you can manage devices and software by using Microsoft Intune. I will show you how to set up and configure an Intune subscription and how you can use that subscription to help your network users get the most out of the network resources and software.

I will start the chapter by talking about managing devices using Intune. I will show you how to provision user accounts and enroll devices. I will also discuss how to manage and configure devices using the Microsoft Intune subscription.

I will then continue the discussion by showing you how to deploy and configure updates using Intune. I will show you how to use the In-Console monitoring tools and how to approve and decline updates.

I will then talk about working with mobile devices including Windows tablets, broadband metering, and tethering, as well as how to wipe mobile devices for employees who leave the company.

I will then show you how to use Intune to help deploy and maintain your company's software packages. I will also talk to you about sideloading applications into your users' devices and the different types of reports that you can run to check on the various hardware and software in your environment.

Let's get started by discussing how you can use Microsoft Intune to help manage and maintain your corporate devices.

Managing Devices with Microsoft Intune

The first thing we need to discuss in this chapter is exactly what Microsoft Intune is. Microsoft Intune is a device management system (see Figure 6.1). *Microsoft Intune* allows administrators to manage mobile devices, mobile applications, and PC management capabilities all from the cloud.

Administrators using Intune can provide their users with access to corporate applications, data, and resources from almost anywhere and on almost any device while also keeping corporate information secure.

FIGURE 6.1   Microsoft Intune dashboard
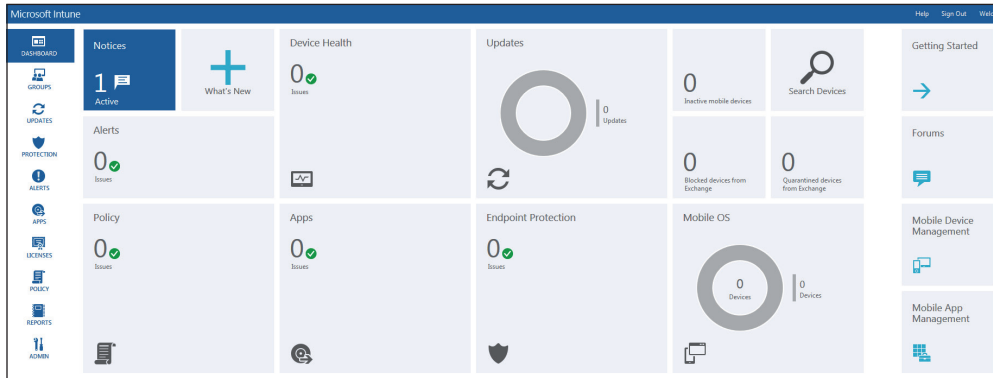
Microsoft Intune also helps you save money because it allows you to license users instead of devices. So if you have a user who works from multiple devices (laptop, tablet, and Windows Phone), you pay only once for the user license instead of multiple times for all of the user's devices.

Administrators can use Microsoft Intune to support and manage Windows 10. Administrators can use Intune on a Windows 10 device for the following:

- Enrollment
- Organization resource access
- Application management
- Policies
- Inventory
- Reporting
- Remote wipe

Microsoft Intune is built on Microsoft Azure Active Directory and System Center. Active Directory is a Directory Services database created by Microsoft. Directory Services was originally designed by Novell, and starting in Windows Server 2000, Microsoft's version—Active Directory—was introduced to the world. To put this in an easy way to think about, Active Directory is just a database that allows administrators to control access to the network.

Microsoft has now taken Active Directory to a new level with cloud-based Active Directory, or Azure Active Directory. Now instead of requiring your organization to buy Windows Server and the required hardware, you can just use a cloud-based version of Active Directory.

> **NOTE** Azure Active Directory will be covered again in Chapters 7, "Configuring Applications," and in even greater detail in Chapter 9, "Configuring Network Connectivity."

Microsoft System Center Configuration Manager allows administrators to have a wide-ranging solution for change and configuration management. Configuration Manager allows an administrator to perform the following tasks:

- Deploy corporate operating systems, applications, and updates
- Monitor and fix computers for compliance requirements
- Monitor hardware and software inventory
- Remotely administer devices

Understanding Microsoft Intune Benefits

Microsoft Intune has many different benefits to help an IT department be more productive and keep its systems running all on the same software. Intune provides an IT department the ability to keep corporate data secure while allowing users to access the same company software from any device that they want to work from. Here are some other Intune benefits:

- Multiple device enrollments for users. Licenses are per user and not per device, so users can work from multiple devices.
- Corporate data security for users and applications like Microsoft Exchange, Outlook, and Office.
- The ability to use Office 365 from any approved device.
- Since Microsoft Intune is a cloud-based system, the IT department is not required to build an infrastructure. This saves the additional cost of buying and maintaining hardware and software.
- Microsoft Intune extends your System Center Configuration Manager through both the cloud and on-premise versions by connecting the two systems together through the use of an application connector.
- Microsoft 24/7 support is available through worldwide phone support or online support. Also, administrators have access to Microsoft.com for Intune FAQs and its knowledge base.
- Corporations have multiple licensing options available to them to choose from. Intune is also part of the Enterprise Mobility Suite by default.

Configuring Intune Subscriptions

When you are deciding about using Microsoft Intune, you must think about the subscription type that you want. You can start with a free 30-day trial or move directly into a full paid subscription. Either choice allows you to start managing mobile devices and corporate computers immediately.

One of the nice advantages to the Intune subscriptions is that if you decide to add at least 150 user licenses, you get to use Microsoft's FastTrack Benefits Center. This benefit also allows a Microsoft specialist to work with your organization. This Microsoft specialist then helps you get the most out of using Intune and all of its benefits.

To start using Microsoft Intune is a very easy and free process. You go out to Microsoft's website and sign up for a free 30-day trial of Intune. Then you start adding your users, groups, and devices. Then if you decide that Microsoft Intune is right for your organization, you can sign up for one of their monthly rates.

Once you have decided to take that next step, you need to start redesigning your company's infrastructure to include the cloud-based subscription. This can be as easy as setting up your DNS servers to include the cloud-based services or as complex as adding all of your devices to the cloud and phasing out many of the infrastructure servers that you currently have running in house.

Whatever you decide, one of the most important phases of moving to a cloud-based system is planning. Once you have made the decision to move to the cloud, that's when the real work happens. Here are some questions to think about:

- Will you be moving all users to Azure Active Directory?

- Will you be using the cloud just for device and software deployment?

- Will you be phasing out in-house equipment?

- Will you allow users to use their own devices (Bring Your Own Device—BYOD)?

- If users use their personal devices, will you supply them with corporate software applications?

- Will you be using Office 2013 or Office 365?

When you sign up for a Microsoft Intune account, you will choose a domain for your Intune subscription. After you sign up for your Intune subscription, Microsoft will send you an email that will have your Intune information contained within the email. Figure 6.2 shows an example of the information contained within the Microsoft Intune email.

In Exercise 6.1, I will show you how to set up a free Microsoft Intune 30-day trial account. You will need to complete this exercise to do some of the other exercises in this chapter.

FIGURE 6.2   Microsoft Intune email
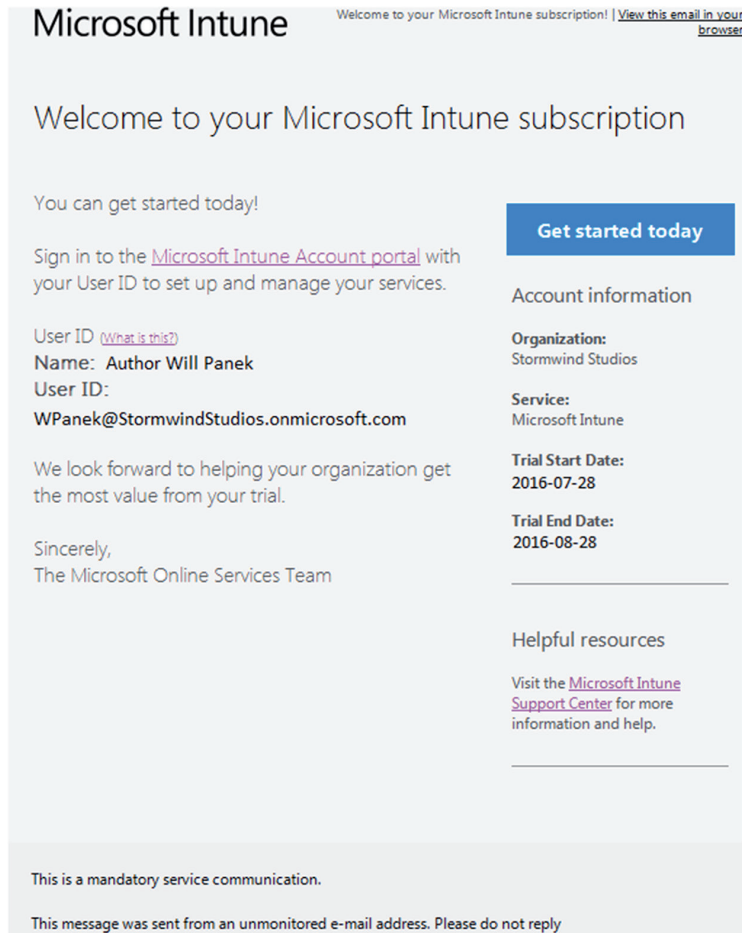
EXERCISE 6.1

Setting Up a Microsoft Intune Account

1. Go to the Microsoft Intune website (`http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/overview.aspx`).

2. Click the Try Now button.

3. On the Welcome to Microsoft Intune page, fill out the required information (Country, First Name, Last Name, etc., as shown in Figure 6.3), and then click Next.

FIGURE 6.3   Microsoft Intune signup

4. On the Create Username screen, create a username and password. Click Next.

5. You will need to prove you're not an Internet robot by verifying your account. Type in a cell phone number so that a verification code can be texted to you. Then enter the code and click Verify. Then click the Create my Account link.

6. You will get a screen with a link to your portal and your username. Print this page for later use.

7. Type the portal link into your web browser and then enter your username and password.

8. In the lower-left corner of the Menu window, click the Intune link to bring up the Intune dashboard.

Provisioning User Accounts

Once you have decided to sign up for the Microsoft Intune subscription, you next need to start assigning your corporate users and groups to Intune. By assigning users and groups, you are choosing which individuals get to access the cloud-based services of Intune, and the IT department gets to start using all of the Intune benefits.

As stated previously, once you sign up for the Microsoft Intune subscription, you will receive an email with your user information along with a link to the Microsoft Intune portal. Click that link and then sign in. Once you sign in, you will automatically be redirected to the Intune Dashboard. This is where you can start creating your users and groups.

During the Microsoft Intune subscription process, you create a domain name, and that domain is added to a Microsoft extension by default. So, if I choose a domain named Stormwind, then the default Microsoft subscription will look like Stormwind.onmicrosoft.com. If your company already owns its own domain name, then you can use that domain instead of the default Microsoft option.

Setting Administrator Accounts

Be sure to decide which way you want to set up your cloud-based domain because if you decide to use Microsoft's default, all of your users will end up with an onmicrosoft.com extension for their User Principal Names (UPNs). Using a pre-owned domain name can make your life in IT much easier because your users will log in using the same domain name that they are using now on a daily basis.

When setting up your Azure Active Directory, you can have this cloud-based version of Active Directory work with the on-premise server-based version of Active Directory by using the Azure Active Directory (AD) Connect tool (formerly known as the Directory Synchronization tool, the Directory Sync tool, or the DirSync.exe tool).

> **NOTE** You can download the Azure Active Directory Connect tool from the Microsoft website `https://www.microsoft.com/en-us/download/details.aspx?id=47594`.

The Azure Active Directory (AD) Connect tool is a server-based application that can be installed onto a server that is currently joined to your local domain. The connect tool allows your corporate onsite users to synchronize to your cloud-based services.

When you decide to connect your Azure Active Directory to your onsite server-based Active Directory, user administration becomes much easier for your IT department. It allows your users to use a single sign-on to access both the local resources and the cloud-based resources. When users have to log in using different accounts, it puts more stress on an IT department and/or help desk.

The first users that you should add to Microsoft Intune are your administrators. By adding the administrators first, then they can start to help also build other user accounts. When you are choosing administrative privileges, you can choose from three administrator types: Tenant Administrator, Service Administrator, or Device Enrollment Manager. Let's take a look at each of these administrator's permissions.

Tenant Administrator

Organizations have the ability to set an administrator up as tenant administrators. Tenant Administrators are used for very specific tasks. Normally, Tenant Administrators are assigned only one dministrator role. This one administrative role determines the

administrative scope for the user and the tasks they can manage. Tenant Administrators can be any of the following roles:

Billing Administrator   The Billing Administrator makes purchases, handles company subscriptions, manages support items, and handles service health issues.

Global Administrator   The Global Administrator has the ability to access all administrative features. By default, the administrator who signs up for the Intune subscription is the Global Administrator for your organization.

- Global Administrators are the only administrators who can assign other administrator their rights.

- Organizations have the ability to have more than one Global Administrator within your organization.

Password Administrator   Password Administrators have the ability to deal with user password issues like resetting passwords, managing requests, and monitoring service health. Password Administrators are allowed to reset passwords for users and other password administrators.

Service Support Administrator   Service Support Administrators can manage service requests, and they can handle service health requests.

User Management Administrator   User Management Administrators can deal with user issues like resetting passwords, handling service health requests, and managing user accounts and groups.

Service Administrator

This is a tough role to truly understand because Intune doesn't assign a Service Administrator role. Actually, the Service Administrator role is just a Tenant Administrator role with the Global Administrator permission assigned to the individual who signed up for the Microsoft Intune subscription. Service Administrators use the administrative console to handle the daily tasks for Intune.

Device Enrollment Manager

One of the great benefits of using Microsoft Intune is the ability of users to enroll multiple devices. By default, each user can enroll five devices if they want. If you want a user to help other users enroll devices, then you can also make a user a Device Enrollment Manager. This role allows an administrator or user the ability to enroll devices for other users. This is also useful for companies that have kiosk-type machines. Your Device Enrollment Manager can enroll these types of systems.

Creating a User in Intune

Once you have decided to use Microsoft Intune, you must start setting up user accounts within Intune so that your users can start accessing the benefits of using Intune.

For users to access Intune, they must have a valid license. When a user has a valid user license, they can then enroll up to five of their devices. This way they can use different devices to do different tasks from both work and home.

When adding users into the Intune portal, you can do it either one user at a time or by bulk import from a CSV file. When adding users, you must assign licenses to each of these users. No matter how you add a user, adding a license to that user is not necessary at the time the user is created. But a license must be associated to that user before that user can access Intune.

If you decide to import your users from your on-site Active Directory to the cloud, the users will *not* have a license. You will be required to assign licenses to your users after the Active Directory merger to Intune.

Let's take a look at how easy it is to create a new user. In Exercise 6.2, I will walk you through the process of creating a new user in the Intune Management Console.

EXERCISE 6.2

Adding Users into Microsoft Intune

1. Open the Microsoft Intune portal by clicking the link in the email that you received from creating your subscription in Exercise 6.1.

2. Once you're in the Intune Dashboard, click the Users link under Management.

3. In the center of the console under Users, you will see a New button with a down arrow. Click New and choose User (shown in Figure 6.4).

FIGURE 6.4   Intune new user
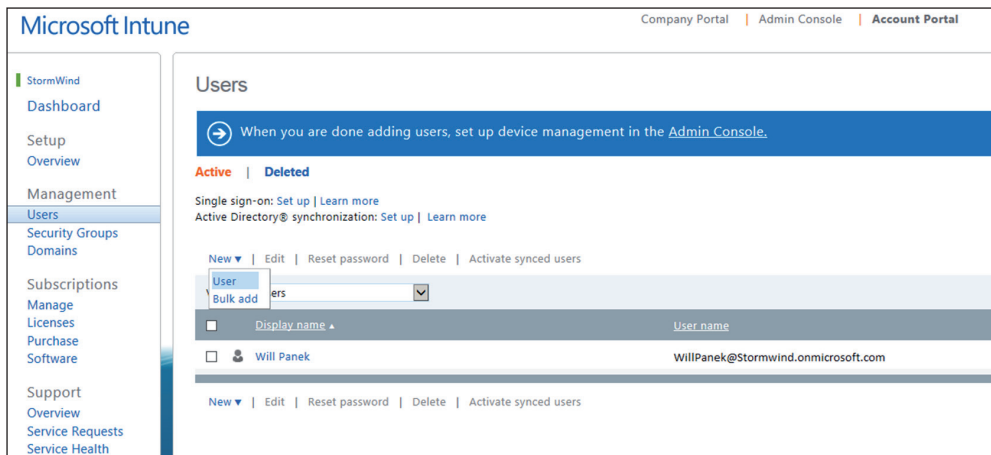
4. If you are asked to re-log back in, enter your Intune username and password.

5. On the New User Details screen, enter the user's First Name, Last Name, Display Name, and Username (see Figure 6.5). Click Next.

FIGURE 6.5   Intune New User Details

6. On the Assign Role screen, you must decide if this new user should have administrative rights and which type. You can choose Yes or No on this step. (I chose Yes, gave the user global administrator privileges, and set up an email address for administrative emails.) Click Next.

7. At the Group screen, just click Next. You will add users to a group in another exercise.

8. At the Send Results In An Email screen, make sure there is an email address for this user and click Create.

9. At the Results screen, print out the user's temporary password (see Figure 6.6). Click Finish.

FIGURE 6.6   Intune New User Results page

10. Close the Intune portal.

Now that we have looked at creating a user in the Intune Management Console, let's take a look at how to create device groups.

Creating Device Groups

Creating groups in Intune helps administrators have more flexibility when it comes to Intune management. Administrators can set up groups based on devices, users, geographic locations, departments, or even hardware types.

There are two main types of groups in Microsoft Intune: device groups and user groups. The groups are created in about the same way, but deciding which groups to create is when the planning and decision making takes place.

When creating new device groups, you can choose which types of devices you want to manage. For example, you can choose mobile devices or all devices. Also, when creating groups, you must add your groups to a parent group. For devices, the parent group is called All Devices. As you create more groups, those groups can become parent groups to other groups.

> **NOTE** It is very important to understand that when you create a child group off a parent group, that child group can't be moved to another parent group without deleting the group. So for example, let's say that I have a group called Corporate and a group called NH. If I create a child group called Portsmouth under Corporate and then want it to be a child group off the NH group, I have to delete the Portsmouth group and re-create it under NH. It's important to understand that when you delete groups, the users do *not* get deleted when the groups get deleted.

Administrators create device groups to help deploy applications and updates to specific devices. In Exercise 6.3, I will show you how to create a device group using the Microsoft Intune Management Console.

EXERCISE 6.3

Creating a Device Group

1.   Open the Microsoft Intune portal and sign in.

2.   In the Intune Management Console, click the Groups link on the left side.

3.   In the window on the right, under Tasks, click the Create Group link (shown in Figure 6.7).

FIGURE 6.7   Choosing the Create Group task
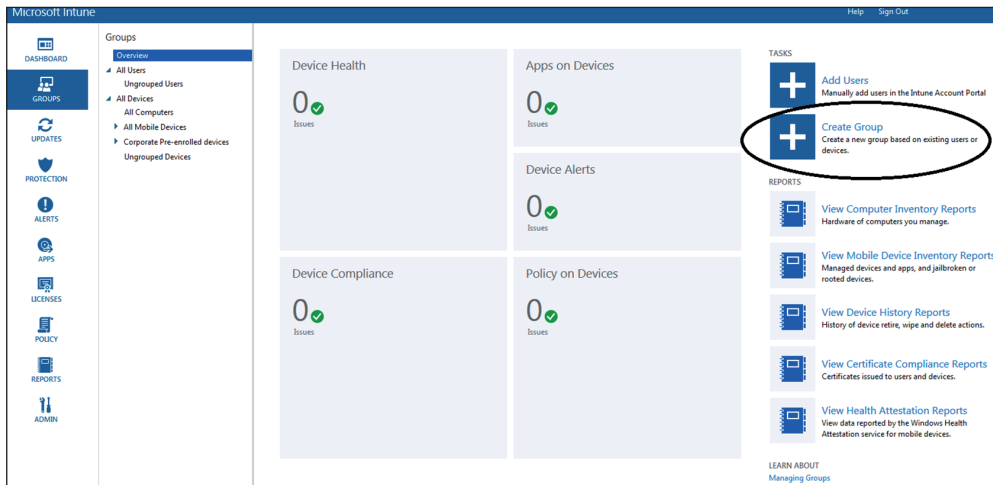
4. At the Create Group screen, under Group Name type **My Devices**. You can add a description to the Description section. Under the section called Select, choose a parent group, click the All Devices choice, and then click Next.

5. At the Define Membership Criteria screen, choose what type of devices you want to include. For this exercise, we are changing the device type from Mobile to All Devices. Click Next.

6. At the Define Direct Membership screen, you can include or exclude devices from this group. Since this group was created using all devices, we are not going to exclude anything. Just click Next.

7. At the Summary screen, verify that everything is correct and click the Finish button (shown in Figure 6.8).

FIGURE 6.8   Create Group Summary screen
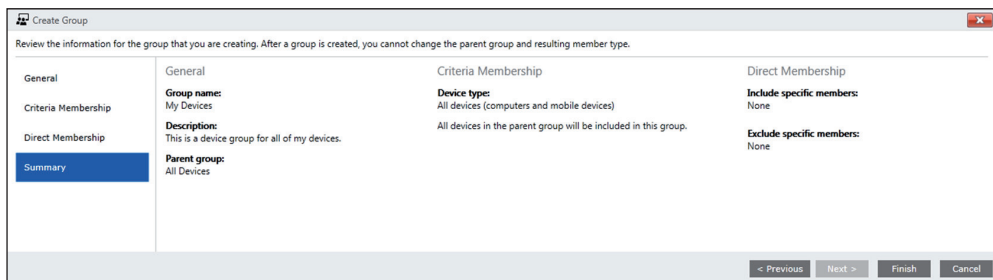
After you create the group, you can view and manage it from the Intune administrative console. You can change the group properties, and you can add or exclude devices from this group at any time. Managing and maintaining the device groups is easily accomplished from the Intune administrative console.

Now that you have created a device group, let's look at how to create a security group.

Creating User Groups

Creating user groups is not much different than creating device groups. User groups allow administrators to manage users by position type, geographic location, or even by hierarchy (executives, directors, managers, etc.).

When creating new user groups, you can choose which parent group you want your group to be part of. For users, the default parent group is called All Users. As you create more groups, those groups can become parent groups to other groups.

In Exercise 6.4, I will show you how to create a user group called Intune Users.

EXERCISE 6.4

Creating a Security User Group

1. Open the Microsoft Intune portal and sign in.

2. In the Intune Management Console, click the Groups link on the left side.

3. In the window on the right, under Tasks, click the Create Group link.

4. At the Create Group screen, under Group Name type **Intune Users**. You can add a description to the Description section. Under Select A Parent Group, click the All Users choice and then click Next.

5. At the Define Membership Criteria screen, choose what type of users you want to include. For this exercise, we are using All Users in the Parent group. Click Next.

6. At the Define Direct Membership screen, you can include or exclude users from this group. Since this group was created using all users, we are not going to exclude anyone. Just click Next.

7. At the Summary screen, verify that everything is correct and click the Finish button.

After you create the security group, you can manage that group from the Intune administrative console. Administrators have the ability to change the group membership at any time. Managing and maintaining the security groups is easily accomplished from the Intune administrative console.

As I stated in the previous note, when you create a child group off a parent group, that child group can't be moved to another parent group without deleting the group. Remember, when you delete groups, the users do *not* get deleted when the groups are deleted.

Now that you have seen how to create users and groups in Intune, let's look at how to set up Intune policies.

Creating Intune Policies

Administrators have the ability to place rules on security settings, firewall settings, and endpoint protection settings on their Intune mobile devices and applications. Think of Intune policies as network Group Policies. These are rules that you can put on devices or users.

Once you decide to move to Microsoft Intune for your devices, it's important to use Intune policies to help manage the devices on your network and set up endpoint protection. Microsoft Intune helps your IT staff deploy devices and applications, and Intune policies allow the IT team to manage the settings on these deployments. When you build a policy, you can deploy that policy to the user groups that you set up in the previous section. Then when the user logs in to Intune, the policy becomes their baseline policy.

You can create policies for the different types of devices available for Microsoft Intune. You can create policies for Android, iOS, Mac OS X, Windows, software, Computer Manager, and common mobile device settings.

In Exercise 6.5, I will walk you through the steps required to set up a Microsoft Intune policy. Administrators have the option to change the policy at any time.

EXERCISE 6.5

Creating an Intune Policy

1. Open the Intune administration portal.

2. In the left pane, click the Policy icon (see Figure 6.9).

FIGURE 6.9   Policy screen
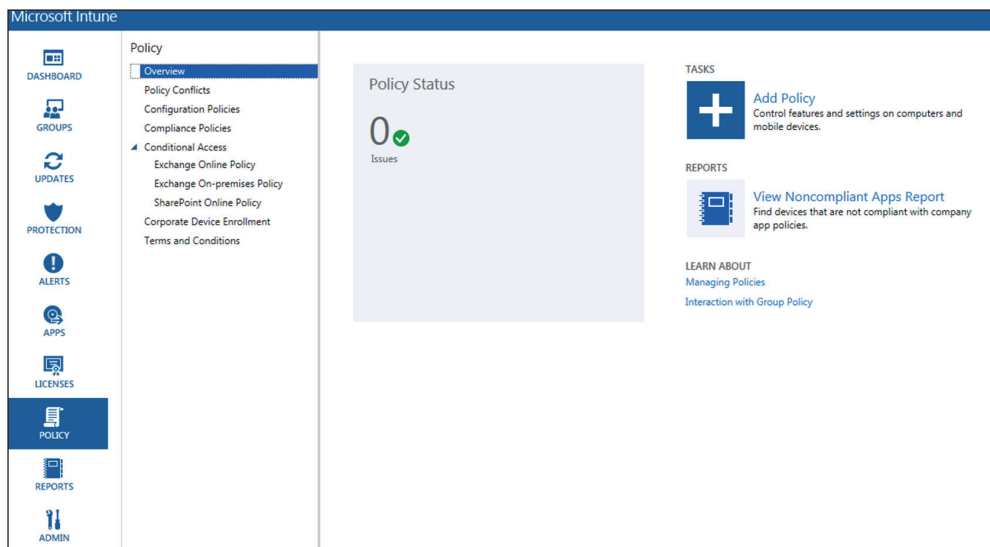
3. In the Tasks section on the Policy Status page, click the Add Policy link.

4. In the policy list, expand the platform you want to create a policy for; select Windows ➢ General Configuration ➢ Windows 10 Desktop And Mobile And Later. Under the General Configuration section, click the Create And Deploy A Custom Policy radio button. Then click the Create Policy button.

5. In the Create Policy window, type in a policy name and description. Then choose which policies you want to enforce under the Password, Encryption, System, Cloud, Applications, Apps, Device Capabilities, Hardware, Features, and Update sections. Click the Save Policy button.

6. If prompted to deploy this policy now, click the No button. If you want to deploy the policy, go ahead and click Yes, but for these exercises we do not want to configure live settings in a test environment.

7. To apply the policy to a user or device group, click the policy and then right-click the policy and choose Manage Deployment.

8. When prompted to select the groups to which you want to deploy this policy, select Intune Users from the previous exercise, and click Add. Then click OK.

Now that we have looked at how to set up Intune users, groups, and policies, it's time to look at how an administrator enrolls devices in Intune.

Enrolling Devices Using Intune

To take advantage of using Intune, you must enroll devices into the Intune system. To enroll clients into this system, you must download the Intune client software onto the devices that need to be enrolled.

For some of the devices on the market today, you may need to take additional steps in order for them to work with your Intune network. For example, to use the Apple iOS, an Apple Push Notification service (APNs) certificate must be imported from Apple so that you can manage iOS devices. This certificate allows Intune administrators to manage iOS.

When an administrator goes to enroll the many different devices on the Intune network, as stated, some of the different devices require different installation options.

Apple iOS   Administrators need to import an Apple Push Notification service certificate from Apple so that you can manage iOS devices. Administrators need to open the Microsoft Intune administration portal and go to Administration ➢ Mobile Device Management ➢ iOS and Mac OS X ➢ Download the APNs Certificate Requests (see Figure 6.10). Administrators then must save the certificate signing request (.csr) file locally. The .csr file is used to request a trust relationship certificate from the Apple Push Certificates Portal. The administrator then needs to click the Upload The APNs Certificate.

FIGURE 6.10 Upload An APNs Certificate screen
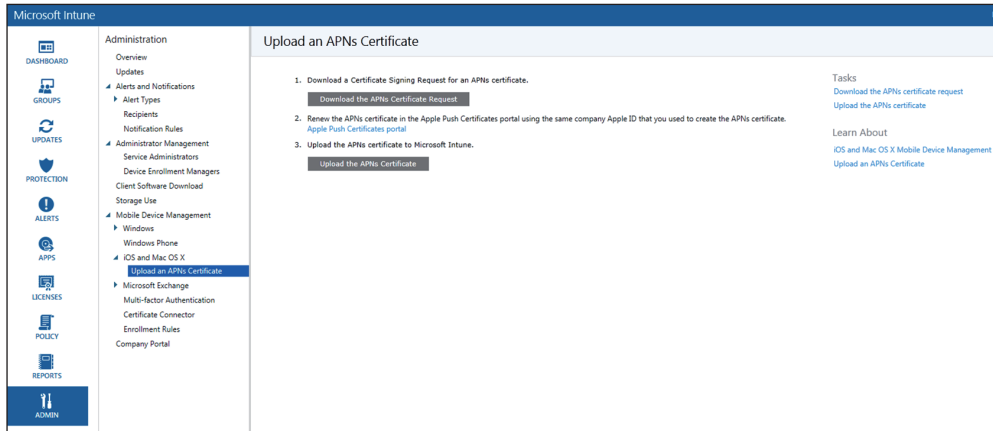
Android Devices No additional configurations in the Intune console are needed to enable Android mobile device enrollment.

Windows Phone Administrators must set up some management requirements before Windows Phones will work with your Intune network. DNS administrators need to create CNAME records in order for users to connect to the Intune network resources. Windows Phones also require a certificate to establish encrypted communications between the client device and the Intune cloud-based system.

Windows Devices Windows devices are connected basically the same way as Windows Phones. The DNS administrator has to create a CNAME record, and then applications can be sideloaded into the Windows computer. Users can also connect to Intune by using the Intune Management Portal.

> **NOTE** Sideloading applications using Intune will be explained in greater detail later in this chapter. Sideloading basically means loading pre-bought or company applications using the Windows Store, Intune, or images.

Administrators can use the Mobile Device Management (MDM) tools to help your company users enroll different devices and manage their Intune accounts. MDM provides the following benefits:

- MDM gives users the capabilities of enrolling their own devices through the use of the self-service Company Portal app. After users enroll their devices, they can install corporate applications.
- Once a device is enrolled, MDM helps deploy certificates, Wi-Fi, VPN, and email profiles automatically. This allows users to have access to corporate resources with the necessary security configuration options.

- MDM allows administrators to use broad management tools for managing mobile devices, passcode resets, device lockouts, and data encryption and to fully wipe a stolen device to help protect against corporate data loss.

- MDM helps simplify the enrollment of corporate devices using bulk enrollment tools like the Apple Configurator.

- MDM allows administrators to easy enroll Apple iOS devices with the Device Enrollment Program (DEP).

- MDM allows administrators to enforce a much stricter lockdown policy for iOS, Android, and Windows Phone devices.

To enroll clients into the Intune network, you can install the software in a variety of ways. The company administrator can provide an installation package to allow users to enroll their systems. Administrators can set up a Group Policy that can be used to enroll the computer into Intune, or users can self-enroll using the Intune portal.

If you decide to use MDM, you must first set up the mobile device management authority. This enables management of device platforms and allows your devices to be enrolled via the Company Portal app.

In Exercise 6.6, I will walk you through how to install and enroll your Windows 10 laptop or desktop in Microsoft Intune.

EXERCISE 6.6

Enrolling a Device in Intune

1. Enter the address of the Microsoft Intune portal into your web browser.

2. Click the Enroll button (see Figure 6.11).

FIGURE 6.11   Enroll screen
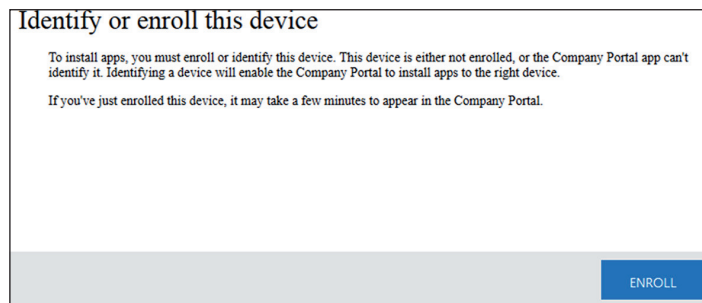
3. On the Enroll Your Computer screen, click the Download Software button (see Figure 6.12).

FIGURE 6.12   Download Software button

Enroll your computer

Enrolling your computer installs the Microsoft Intune software.

Microsoft Intune may impact other software and allows your technical support administrator to enforce security policies on your computer. Learn more about Microsoft Intune.

Note: You must have administrator permissions on this computer to install this software. View the system requirements.

DOWNLOAD SOFTWARE

4.   If the Save As box appears, click the Save File button (see Figure 6.13). If the download automatically starts, go to step 5.

FIGURE 6.13   Save File dialog box

Opening Microsoft_Intune_Setup.exe

You have chosen to open:

  Microsoft_Intune_Setup.exe

    which is: Binary File
    from: https://msua05.manage.microsoft.com

Would you like to save this file?

Save File   Cancel
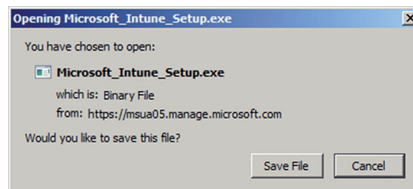
5.   Once the file is downloaded, click the Run button.

6.   The Microsoft Intune login screen will appear, as shown in Figure 6.14. Log into Microsoft Intune.

FIGURE 6.14   Microsoft Intune login screen
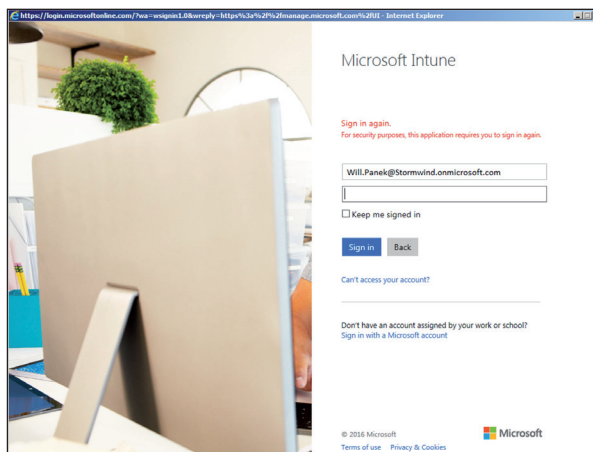
7. On the Welcome To Microsoft Intune Setup Wizard screen, click Next (see Figure 6.15).

F I G U R E   6 . 1 5   Welcome to Microsoft Intune
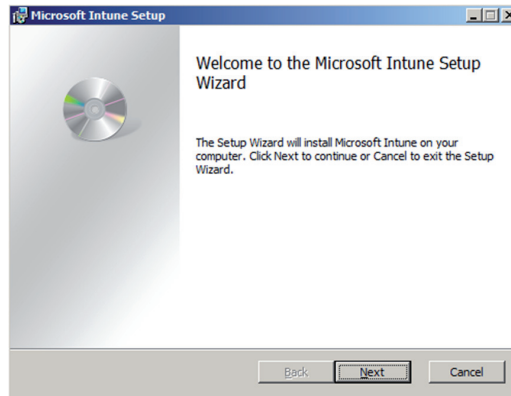
8. Microsoft Intune will be installed. If a User Account Control box appears, click Yes.

9. On the Complete screen, click the Finish button.

10. Log back into the Microsoft Intune portal.

11. If the message states that the computer is still not recognized, click the message. A box will appear, asking if you now want your computer to be enrolled. Click the radio button next to your system name and click the Select button, as shown in Figure 6.16.

F I G U R E   6 . 1 6   Select your device
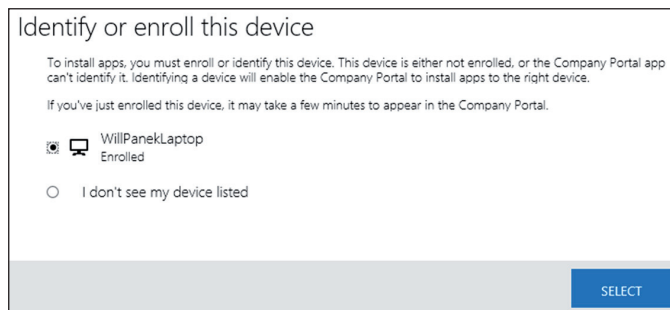
12. If you refresh your Intune portal, you will see your newly connected device. Click the device and it will show you the device settings, as shown in figure 6.17.

FIGURE 6.17   Device Settings in Intune
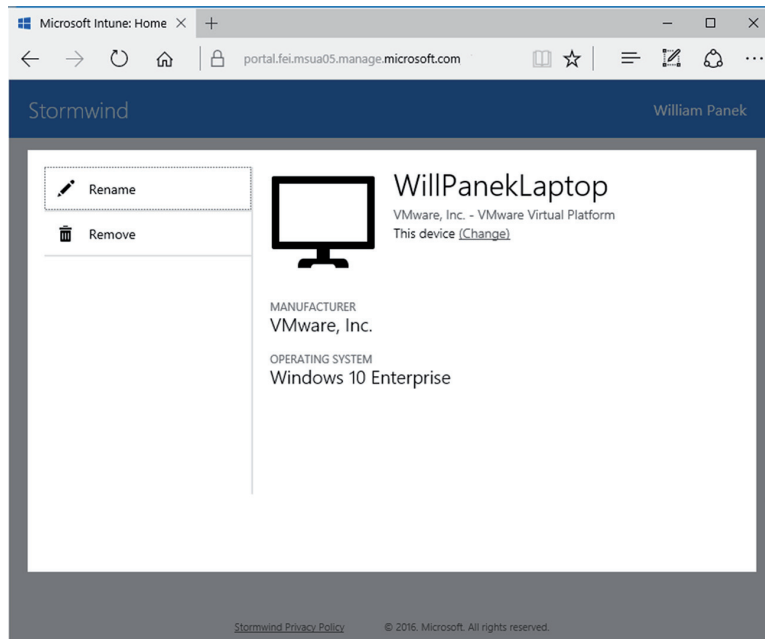
13. Close the Intune portal.

Configuring the Intune Connector Site

To understand how connectors work, you must first understand what a connector does and why we use them in the computer industry. Connectors allow different types of devices to communicate with each other. So, for example, let's say you had a Microsoft Exchange server and a UNIX-based mail server. You would add a connector into the Exchange server so that it could communicate and understand the UNIX mail server. That's how Intune connectors work also.

Intune connectors allow Microsoft Intune to communicate and understand other types of devices and software. So if you decide to use Azure Active Directory and Azure Exchange, you can install a connector so that Azure Exchange can work with the corporate Exchange mail server.

Exchange devices have the ability to be managed through both the on-premise Exchange servers and the hosted Exchange servers in the cloud. The Exchange connector connects your users with your Exchange deployments, and the connector lets you manage your mobile devices through the Intune console.

Administrators who have been using System Center Configuration Manager to manage their computers, Macs, and UNIX-based devices can add the Intune connector so that they can manage all of these devices from one console.

To configure connectors, in the Intune Management Console click the Admin link. Then expand the Mobile Device Management section. You would then click the device or software package and set up the connector.

Configuring Intune Alerts

One of the advantages of using Intune is the ability to monitor and see alerts within Intune. There are different levels of severity within the alerts. Table 6.1 shows you the different alert types and what each type means.

TABLE 6.1   Intune alert types

Alert	Description
🔴 **Critical**	This alert shows you that you have a serious issue that needs to be investigated and fixed.
⚠️ **Warning**	This alert shows you that there may be an issue but that issue is not very serious at this time. These alerts need to be investigated to make sure that they do not become a problem in the future.
ℹ️ **Informational**	This alert shows you that there is some information about a product but it's not a problem. For example, an informational alert may tell you that there is an upgrade to a connector that you have installed.

When dealing with Intune monitoring and alerts, there are a few settings that you can set up to help configure how alerts work. For example, under the Alerts And Notifications section, you can set up recipients who will receive emails when alerts happen.

So if you get a critical error, an email can be sent to an administrator so that the IT department can work on resolving the issue as fast as possible. If you don't set up email alerts, someone will need to monitor the Intune system daily to watch for issues. Intune administrators have the ability to set different email recipients for different alert types. So critical alerts can go to one IT person, and warnings can go to another.

Administrators also have the ability to enable or disable certain alert types. So if you are getting a warning that you know is not going to affect your Intune system, you can disable the warning to remove it completely. This way it's not a message your Intune administrators need to see on a daily basis.

To configure your alerts and notifications, in the Intune Management Console click the Admin link. Then expand Alerts and Notifications. You can then create new alert rules and notifications.

Supporting Applications

Microsoft Intune gives an organization the ability to deploy and maintain software from the cloud. The advantage to this is that the software issued through Intune is licensed to the user and not the hardware. So what this means is that you can deploy a copy of Office to a user using multiple devices, and when that user works on corporate data, that data is secure. That's the real advantage to Intune. This allows your users to work securely from their iPhone, Windows laptops, or tablet.

Microsoft Intune also allows an organization to use their current business apps by using the Intune App Wrapping tool. The Intune App Wrapping tool is a command line application that builds a package around the in-house application. Then the business application can be managed by the Intune mobile application management policies.

The Intune App Wrapping tool also gives you secure data viewing through the Intune Managed Browser, AV Player, Image viewer, and the PDF viewer. Administrators also have the ability to deny specific applications or web addresses from being accessed from specific types of mobile devices. Finally, when dealing with corporate data and security, administrators have the ability to wipe out a device in the event that the device is stolen, the device is lost, or the employee leaves the company.

Deploying Applications Using Intune

The way that we do business in the corporate world continues to change on a daily basis. Today, many of our users bring in their own devices. Because of BYOD, it is getting harder for IT departments to deploy software.

As stated earlier in this chapter, Microsoft Intune (Figure 6.18) is a cloud-based desktop and mobile device management tool. Intune helps IT departments provide their users with access to company applications, data, and resources. The users have the ability to access these resources from any type of device (i.e., Apple, Android, or Windows devices).

FIGURE 6.18   Microsoft Intune
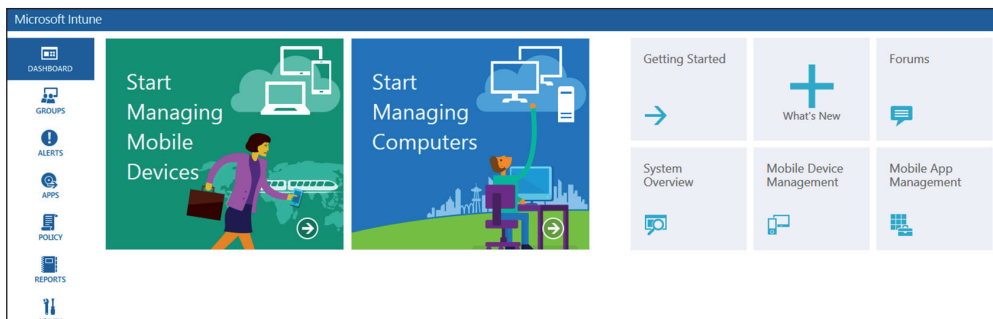
One of the issues that we face as IT administrators is that we have multiple copies of software throughout a company and multiple version types (Apple versions of Office compared to Windows versions). Let's take a look at Office as an example. Many times we have older versions of Office (Office 2010) and newer versions of Office (Office 2016/Office 365).

This is where Microsoft Intune can help out an IT department. You can upload software packages to Intune and your users can get current copies of the software from the web. Also, Intune helps your organization protect its software by giving you extra security and features. Intune also allows you to set up application management policies that allow an IT department to manage applications on different devices.

As long as a device is compatible with Microsoft Intune, you can deploy the applications to that device. Depending on the device and the application, deployment options may vary. Administrators have the ability to upload their applications to Microsoft Intune or link a Windows Store application to Microsoft Intune storage.

To deploy applications using Intune, you must use the proper software installation type based on the different devices that your users may be using. Microsoft gives you a trial subscription of 2 GB of cloud storage. You can purchase more storage depending on how much money you want to spend.

Intune Software Publisher

To make an application available for your users to deploy, you must upload the installation package and then publish the package. As soon as you add or modify an application to Microsoft Intune, the Microsoft Intune Software Publisher starts. Then from the publisher you can choose and configure the software installation type.

To use the Microsoft Intune Software Publisher, you must have Microsoft .NET 4.0 installed on the Windows system. After you install .NET, restart the system and you should be able to use the Microsoft Intune Software Publisher.

Sideload Apps by Using Microsoft Intune

Sideloading an application means that you are loading an application that you already own or one that your company created into a delivery system (i.e., Intune, Microsoft Store, or images).

You may be familiar with sideloading apps into the Windows Store. This is the process of building or buying your own application and then adding it to the Windows Store so that all of your users can download and use that app. Sideloading an application into Microsoft Intune means the same thing. You are taking an application that you built or bought and adding it into Microsoft Intune for user downloads.

Think about how you deploy software today. You buy a package and either manually install the software to your users or use some type of deployment package like System Center Configuration Manager. The only difference now is that the application gets loaded into the cloud and can be deployed to any device that is compatible with the application.

When sideloading applications you can use Microsoft Intune or a combination of Microsoft Intune and System Center Configuration Manager. Microsoft has a Windows

Intune connector that allows Intune to work directly with System Center Configuration Manager. Here are the steps required to sideload applications into Microsoft Intune:

1. Upload your application into Microsoft Intune. To do this, click the Add Apps link (shown in Figure 6.19).

FIGURE 6.19   The Add Apps link
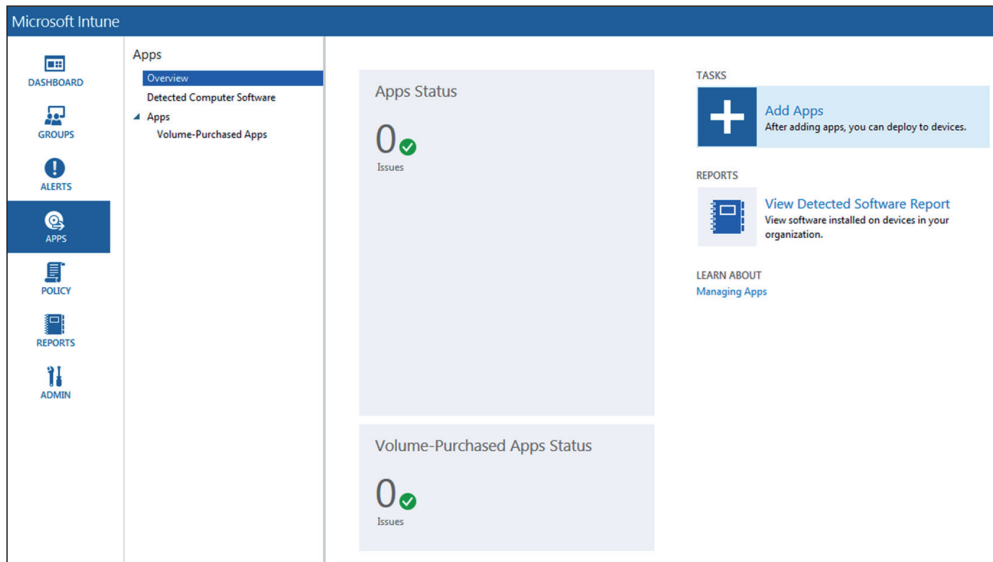
2. A dialog box will appear asking you if you want to download a `setup.exe` file. Click Yes. This is the Microsoft Intune Software Publisher. After it is downloaded, click the exe. The Software Publisher dialog box will appear, asking if you want to install. Click Run (shown in Figure 6.20).

FIGURE 6.20   Install the Intune Software Publisher
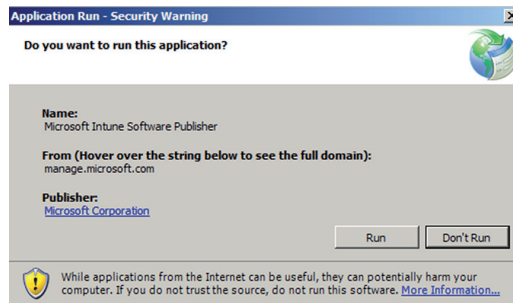
3. The Microsoft Intune Software Publisher sign-in screen will appear. Enter the credentials for a Microsoft account tied to Intune and click the Sign In link.

4. At the Software Setup page, choose the Windows application package software installer type and the Universal Naming Convention (UNC) path to the application.

5. When the Software Description page appears, choose the publisher, user-friendly name, and description of the app. Click Next.

   When the Add Software Wizard is complete, the app will be listed in the Managed Software node in the Software workspace.

Once an application is uploaded to Intune, the next step would be to deploy the application to your users. To deploy the application to the users, you assign the application to the created Windows Intune groups. While in the Windows Intune portal, you would click the Apps link and then choose the app for deployment. The following steps describe how to deploy the application:

1. Open the Microsoft Intune administrator console and click the Apps link.

2. Select the application that you want to deploy, and then click the Manage Deployment link.

3. Choose the user or device groups that you want to deploy the application to.

4. On the Deployment Action page, configure for approval (Required, Available, Not Applicable, or Uninstall) or deadline (when the application must be installed).

5. If the application that you are deploying has the ability to be configured by a mobile application management policy, then the Mobile App Management page will be displayed. On this page an administrator can choose the mobile application management policy that they want with this application.

6. If the application that you are deploying has the ability to be configured by a VPN profile, then the VPN Profile page will be displayed. Here is where you can choose the iOS apps with the VPN profile.

After the application is set up and ready for deployment, an administrator can always go back into the application properties and make changes. To view the properties of an application, click the app and choose the View Properties link. There are three tabs for the software properties.

General   The General tab allows an administrator to see the applications general information and its installation status.

Devices   The Device tab allows an administrator to see the devices that have successfully installed the application.

Users   The Users tab allows an administrator to see the users that have successfully installed the application.

Deep-Link Applications by Using Microsoft Intune

One of the nice advantages of using Windows 10 is that you can purchase Windows store applications. After you purchase the applications, you can deploy the Windows Store application (deep-link) to all of your users.

Supporting Broadband Connectivity

Administrators have a few weapons in their broadband arsenal. Two different options that we can set up as administrators are the ability to see how much network or software bandwidth is being used (metering) and how we can set up our Windows 10 devices to use our cellular Internet connections (tethering).

Understanding Metering

Administrators have the ability to limit and monitor network usage by configuring the network as a metered network. Network metering allows network downloading to be watched or metered, and then administrators can charge users or departments for the network usage.

This is becoming something that many IT departments have started doing due to budgeting. Many IT departments are non-revenue-generating departments, and because of this, it can be difficult for an IT administrator to get a budget passed. But with network metering, you can charge other departments for the amount of bandwidth and network that is being used.

When setting up your company's Internet connection, your ISP has the ability to charge by the amount of data used. That's called a metered Internet connection. If you have a metered Internet connection, setting your network connection to metered in Windows can help you reduce the amount of data you send and receive. To set this up in Windows, you would take the following steps:

1. Click Start ➢ Settings, and then tap Network & Internet.

2. Tap or click the Wi-Fi link and then, under Metered Connection, turn the Set As a Metered Connection option on or off.

Administrators also have the ability to limit how much bandwidth a user or department gets to use when downloading applications. This is referred to as *software metering.*

To set up software metering, an administrator must use a combination of Microsoft Windows Intune and System Center Configuration Monitor.

Understanding Broadband Tethering

Tethering allows a user to use their Windows 10 mobile device through their cellular phone. If you have a Windows 10 mobile device and want it to access the Internet, you can go through your cell coverage to get online.

Tethering can also be connecting one mobile device to another mobile device for Internet access. For example, let's say I have an iPad with cellular Internet connection. I can connect another Windows 10 tablet to that iPad to gain Internet access. So tethering is the ability to connect one device to another for Internet access. Before you set up tethering, here are a few things that you should know:

- There may be extra charges when connecting your data connection with another device.

- Applications and updates may not be downloaded over a metered connection, and by default, tethered and mobile broadband connections are metered.

- Many cellular carriers require that you pay an extra fee for allowing your phone to be a hotspot for tethering. To enable tethering on most devices, you set up your mobile device as an Internet hotspot.

Understanding Data Synchronization

Data synchronization allows you to synchronize your devices with your servers. These servers can be network-based or cloud-based. Administrators have the ability to synchronize work folders, and they can also use the Sync Center to use one application for all of their synchronization needs.

To enable synchronization on the Windows 10 device, click the Start button and choose Settings. When you are in the Settings window, click the Accounts link to set up your user accounts and synchronization (see Figure 6.21).

FIGURE 6.21 Data synchronization
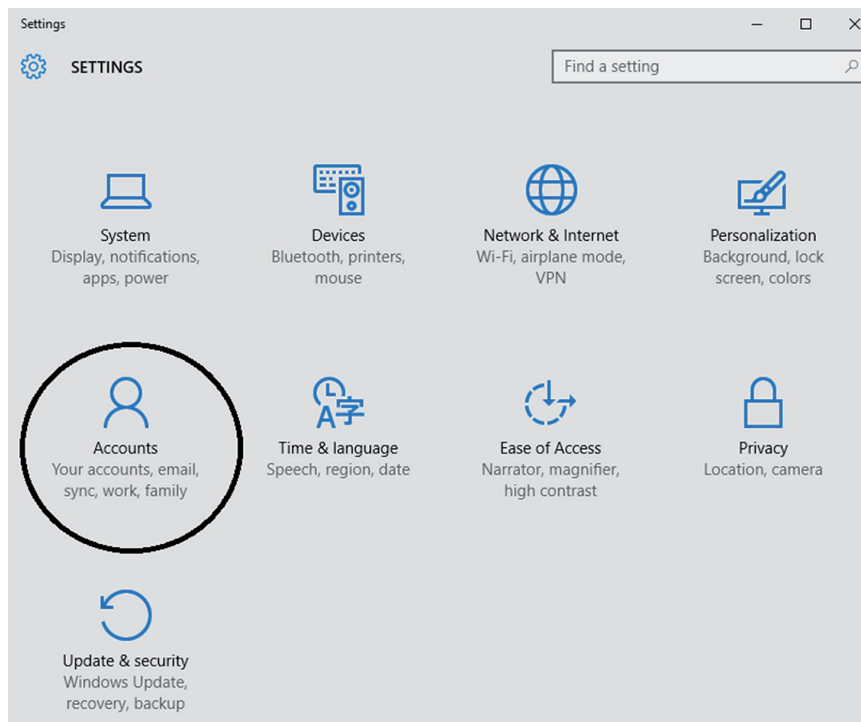
Once you enter into the Accounts link, you can choose the bottom option (Sync Your Settings) to set up all of your synchronization settings (see Figure 6.22).

One of the final things that you want to look at in the Accounts link is the Work Access link. The Work Access link allows you to connect your device to your work or school, sign in to Azure, and enroll in device management (see Figure 6.23).

FIGURE 6.22 Sync Your Settings
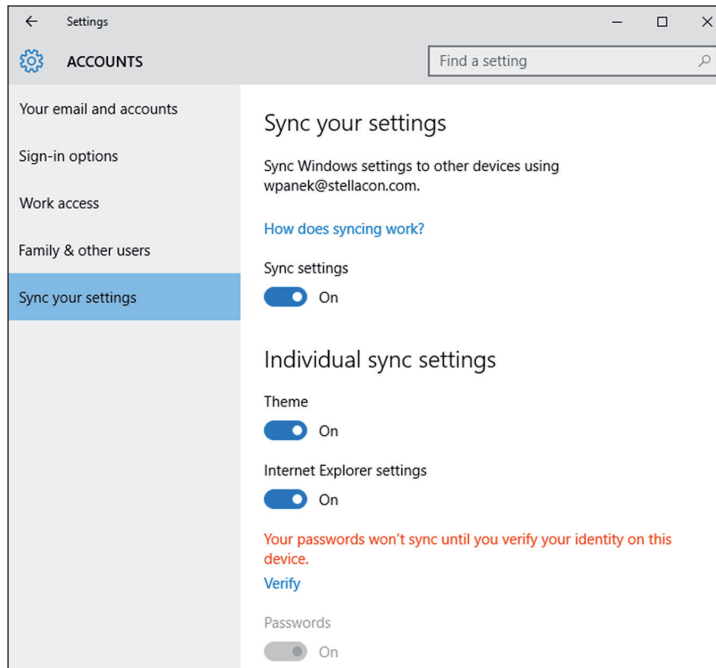
FIGURE 6.23 Work Access link
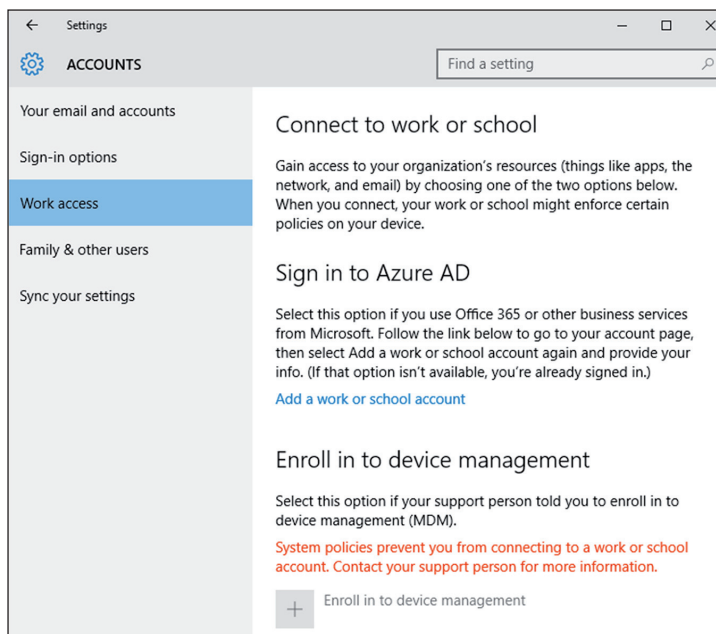
Understanding Updates

Deploying updates can be a very difficult process for many organizations. Depending on the number of users that you have and the number of applications that each user uses, updates can be a very time-consuming process.

Many organizations install a Microsoft server called Windows Server Update Services (WSUS). WSUS servers allow administrators to deploy Microsoft product updates to computers that are running the Windows operating system. Administrators can manage all of their organization's Microsoft updates from one application.

The downside to WSUS is that it is used for Microsoft updates. So you can deploy updates to all of your applications, Microsoft and Non-Microsoft, by using the Intune management portal.

Deploying Software Updates Using Intune

When you decide to use Intune to deploy your updates, you get a lot of options that you get to consider and set up. For example, do you want to approve all of your updates or do you want the updates to automatically deploy? Many administrators like to approve all of their updates so that they have a chance to test them first before deploying.

As updates become available from Microsoft or from any third-party software vendor that your company is using, a notification will be displayed on the Overview page of the Updates workspace (see Figure 6.24).

FIGURE 6.24   Overview of update types
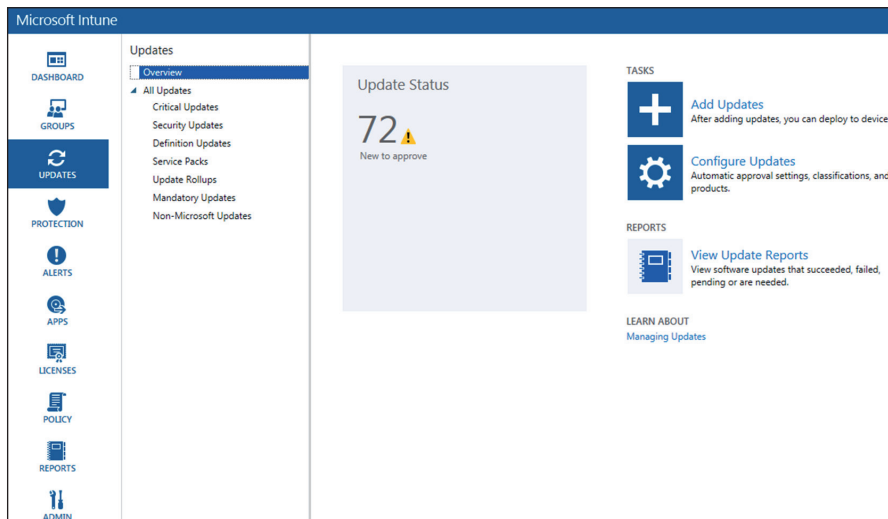
Once an administrator sees these notifications, they can click the notification link and view the information about the update. After viewing the update information, the administrator can then decide if they want to approve or deny the update.

If you have been in the IT industry long enough, you have run into the situation when you did a software update and then the software stopped performing properly. Now, with the ability to test and approve updates in Intune, you can solve this issue. You can guarantee that the update will work as needed or deny the update from being deployed.

This is just one of the options that you have when using Intune updates. Let's take a look at some of the other settings that you need to plan out before setting up your Intune updates.

Identifying Required Updates

When you decide to use Intune for updates, you need to decide which type of updates that you want to install. Administrators have the ability to choose what type of updates they want to install.

All Updates   The All Updates section means just that, all updates. Every possible update that can be deployed will be shown under the All Updates section.

Critical Updates   Critical updates are updates that are released to fix a specific issue that is for a critical bug that is not security related.

Security Updates   Security updates are updates that need to be applied to fix a security issue. These security issues are used by hackers to either hack into a device or software.

Definition Updates   Definition updates are normally software updates that contain additions to a product's definition database. Definition databases get used to identify objects that have very specific attributes. These attributes look for malicious code, phishing websites, or junk mail.

Service Packs   Service packs are a collective set of all current hotfixes, security updates, critical updates, and updates. Normally service packs also contain additional fixes for known issues that are found since the release of the product. Service packs may also contain customer requested design changes or features.

Update Rollups   Update rollup updates are current hotfixes, security updates, critical updates, and updates that are bundled together for easy deployment. Update rollups are normally used to target a specific component or software package.

Mandatory Updates   Mandatory updates are updates that are released to either fix or replace a software or hardware issue. Mandatory updates are required to run or the device or Windows system may stop functioning properly.

Non-Microsoft Updates   Non-Microsoft updates are updates for third-party software and hardware devices. These are updates that other vendors release for solving problems or improving their product.

Approving or Declining Updates

One of the best advantages to using any update service is the ability to either approve or deny updates. Plus, having the ability to approve updates gives you the ability to test the updates first.

In today's virtualization world testing updates can be easier than before. It's easy to set up a virtual server just for update testing without spending thousands of dollars on new hardware. Let's take a look at the steps necessary to approve or deny updates:

1. Open the Microsoft Intune administration console. Then click the Updates link ➤ Overview ➤ New to approve.

2. Select any of the updates and then look at the update description at the bottom of the page. Once you know you want to approve the update, click the Approve link on the top of the page. If you want to approve multiple updates at the same time, hold down the Ctrl key as you select each update and then click Approve.

3. On the Select Groups page, select which group you want to deploy the updates to and then click the Add button. Once you done choosing your groups, click Next.

4. On the Deployment Action page, you have two options to choose from. You can either approve or deny the update.

    -   Under the Approval list, Administrators can choose to do the following:

        -   Required Install—Installs the update on the computers that were chosen in the specified group.

        -   Do Not Install—Allows you to use update reporting but the update is not installed.

        -   Available Install—The user has the ability to choose if they want the update to install from the Company Portal.

        -   Uninstall—Removes the update from the computers in the listed group.

    -   Under the Deadline list, administrators can choose to do the following:

        -   None—This choice sets no deadline for the installation of the update, and users can choose to install or ignore the update as long as the update remains in the list.

        -   As Soon As Possible—This choice forces the update to be installed on the computers at the next possible opportunity.

        -   Custom—This choice allows administrators to specify the date and time that approved updates will be installed.

        -   One Week, Two Weeks, One Month—This choice forces the update to install within the specified time period.

5. Click Finish to save the settings.

6. You can check the details pane at the bottom of the All Updates page for information about the updates.

Configuring Automatic Approval

Another option that administrators can set is the ability to automatically configure updates for automatic approvals. To set this up, administrators would complete the following steps:

1. Open the Microsoft Intune administration console. Then click the Configure Updates link.

2. In the Automatic Approval Rules section (see Figure 6.25) under the Server Settings: Updates page, click the New button.

FIGURE 6.25 Automatic Approval Rules
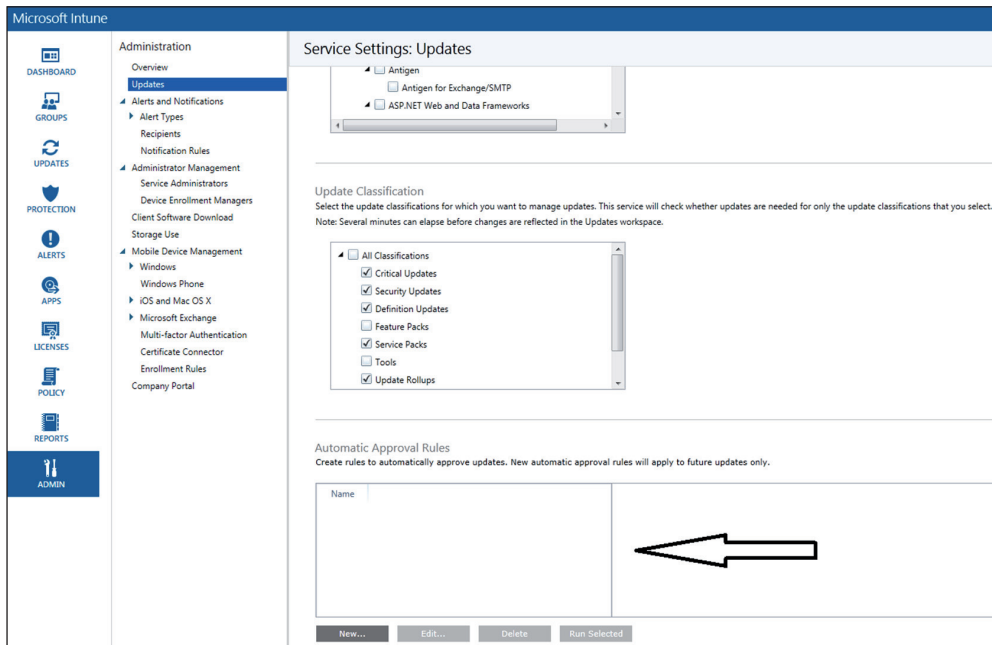
3. On the General page, type in the approval rule name and optional description. Click Next.

4. On the Product Categories page, select the products for which you want to have automatic updates. Click Next.

5. On the Update Classifications page, choose the update classifications that have automatic approval. Click Next.

6. On the Deployment page, choose the devices that these automatic approvals will apply to and click Add. Click Next.

7. On the Summary page, review your settings and then click the Finish button.

Deploying Third-Party Updates

Microsoft Intune has one advantage over using other types of update servers (like WSUS) because Intune can also update third-party non-Microsoft updates. This is very useful when deploying applications like virus protection. The virus list constantly needs to be updated, and Intune can help administrators achieve this.

To deploy software updates to non-Microsoft vendors, you would use the Upload Update Wizard. The Upload Update Wizard helps an administrator get their updates into the cloud storage space. After they are uploaded, administrators can then approve or deny the updates to specific groups. To launch the Upload Update wizard, you would click the Add Updates link (see Figure 6.26).

FIGURE 6.26   Add Updates link
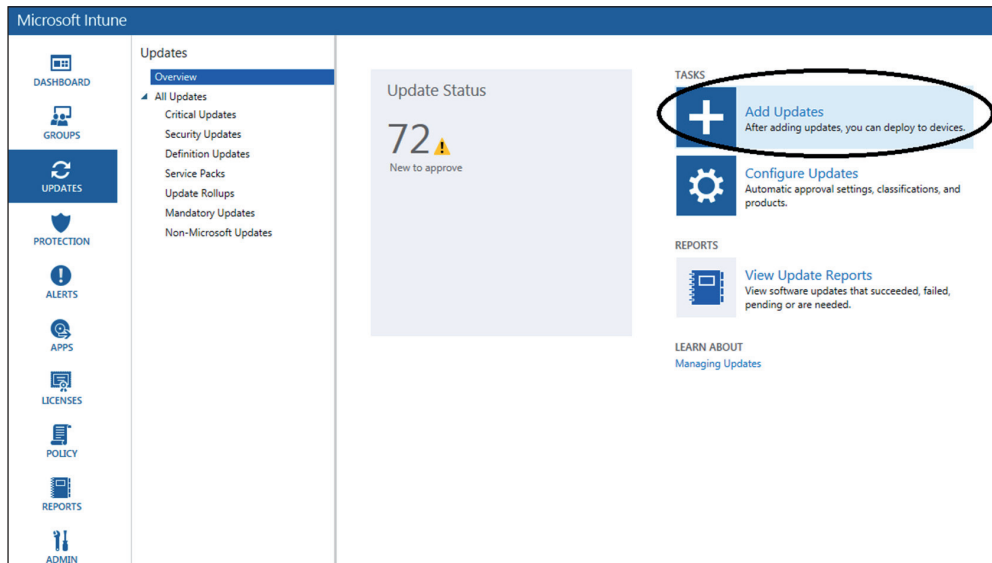
Using the Intune Reports

One of the best tools that Microsoft Intune offers is the ability to obtain all of the different types of reports. The Intune reports help an administrator monitor the status of their enrolled devices and see if there are any issues that need to be addressed. The reports also allow an administrator to examine both the hardware and software inventory.

To access the many different reports available in Intune, you open the Intune Management Console and click the Reports link on the left side (shown in Figure 6.27).

FIGURE 6.27   Reports link
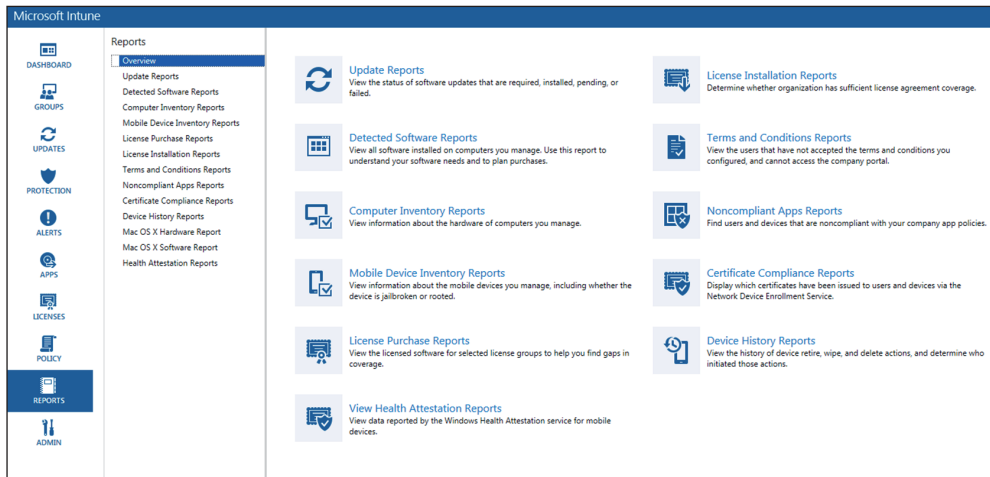
The following descriptions are of just some of the reports that you can run as an administrator to get information about your updates and about your hardware.

Update Report   Running this report allows administrators to see the software updates that were successfully installed on computers in your organization along with information about updates that failed, are pending, or are needed.

Detected Software Report   This report allows administrators to see what software was installed on the computers throughout your organization. This report also includes the software version that was installed. Administrators have the ability to filter the information and display only specific software publishers and specific software categories. Administrators can also get more details by clicking the directional arrow next to the list item.

Computer Inventory Report   Running this report will help administrators get detailed information about the managed computers in the organization. Administrators can use this report for planning hardware purchases and also to get a better understanding about the hardware needs of the users in your organization.

Mobile Device Inventory Report   Administrators can use this report to gather information about the mobile devices in their organization. Administrators have the ability to filter the information that is displayed. Some of this information includes the groups the device belongs to and the operating system that is running on the device.

License Purchase Report   This report allows an administrator to see the software titles for all licensed software in selected license groups. License reports are not an exact list of software that is being used or proof of the software compliance. The report is used by administrators as a tool to help you make licensing decisions for your organization.

License Installation Report   Administrators can use this report to compare installed software with your current license agreement coverage.

Terms and Conditions Report   This report allows administrators to see whether users have accepted the terms and conditions that you deployed and which version they accepted.

Noncompliant Apps Report   Administrators can use this report to see information about users who have applications installed that are on your lists of compliant and noncompliant apps.

Certificate Compliance Report   This report allows you to see which certificates have been installed to users and devices through the Network Device Enrollment Service (NDES). NDES allows hardware, like routers, to be able to receive a certificate even though the router can't request a certificate.

Device History Report   Administrators can use this report to see a historical log of retired, wiped, and delete actions that have been performed. Administrators use this report to see who initiated actions on devices in the past.

Mac OS X Report   This report is run to show you the Mac OS X groups and what software and hardware that they run. This report allows administrators to watch the Apple devices enrolled into the Intune cloud system.

Summary

In this chapter, we talked about the cloud and Microsoft Intune. I showed you how Microsoft Intune can help you manage devices and software. I showed you how to set up and configure an Intune subscription and how you can use that subscription to help your network users get the most out of their network resources and software.

I also talked about managing devices using Intune. I showed you how to provision user accounts and enroll devices. I also discussed how to manage and configure devices using the Microsoft Intune subscription.

I then continued the chapter by discussing how to deploy and configure software and updates using Intune. I showed you how to use the In-Console monitoring tool and how to approve and decline updates.

I then talked about how to work with mobile devices including Windows tablets, broadband metering, and tethering, and I also showed you how to wipe mobile devices for employees who leave the company. I then showed you how to use Intune to help deploy and maintain your company's software packages and updates.

Finally, we looked at the different types of reports that an administrator can run using Intune. These reports can help you see what devices still need updates and also what hardware may need to be installed or replaced.

Video Resources

There are no videos for this chapter.

Exam Essentials

Understand Microsoft Intune.   Understand what Microsoft Intune can do to help your network. Make sure you understand how users and devices get connected to Intune.

Know how to configure a Microsoft Intune Subscription.   Understand how to set up and manage a Microsoft Intune Subscription. Understand how to configure a device to use Microsoft Intune.

Understand the Microsoft Intune benefits.   Understand what Microsoft Intune benefits can be used in a corporate environment. Understand how these benefits, like remote wipe, can help you protect corporate data.

Understand the Azure Active Directory (AD) Connect tool.   Understand that Administrators can connect their cloud-based version of Active Directory (Azure Active Directory) with their on-premise server-based version of Active Directory by using the Azure Active Directory (AD) Connect tool.

Understand Intune Connectors.   Understand Microsoft Intune Connectors allow Microsoft Intune to work with software within a network. The connector allows the cloud-based software to communicate properly with the infrastructure based software.

Understand Intune Alerts.   Understand each type of Intune alerts and which alerts are important to fix immediately or which alerts just are giving you information. Understand how to set up notifications for each alert type.

Know how to work with Intune Reports.   Understand that the different reports help an administrator monitor the status of Intune managed devices. These reports give you information on the status of software updates, software installed, and certificate compliance. Understand how reports also let you examine the inventory of your network's hardware and software.

Review Questions

1. You are the network administrator for your organization. Your users use both desktops and tablets to access the network. Your tablet users use a 4G mobile broadband Wi-Fi connection. You need to watch how much data your users are using on this connection. How do you do that?

    A. Configure the broadband connection as a metered network.

    B. Turn on network resource monitoring.

    C. Enable performance monitor.

    D. Enable tablet metering in the tablets settings.

2. You are the network administrator for a company that has a Microsoft Intune subscription. You have decided to set up three Intune Security groups called CorpGroup, NHGroup, and Portsmouth. CorpGroup is a parent group to Portsmouth. Portsmouth has 75 users in the group. You realized that you need to make NHGroup the parent to Portsmouth. What is the first thing that you need to do?

    A. Edit the security properties of CorpGroup.

    B. Edit the security properties of NHGroup.

    C. Remove all 75 users from Portsmouth

    D. Delete Portsmouth and then re-create the Portsmouth group under NHGroup.

3. You are the IT manager of a large manufacturing company. Sales personnel are allowed to bring their own personal Windows 10 devices to the office. The company allows the sales people to install company software and use their devices to retrieve company mail by using the management infrastructure agent. One of your salespeople reports that their Windows 10 laptop was stolen while at the airport. You need to make sure that no one can steal any of the corporate data or access any corporate emails. Which two actions should you perform? Each correct answer presents part of the solution.

    A. Prevent the computer from connecting to the corporate wireless network.

    B. Remove the computer from the management infrastructure.

    C. Reset the user's password.

    D. Do a remote wipe on the users laptop.

4. You are the IT director for a large school system. The school has decided that students can bring in their own devices to do school work with. Your organization uses Microsoft Azure Active Directory and Intune for all of the student's applications and network authentication. You need to be sure that students that are using IPADs as well as Windows 10 devices have full access. What do you need to do to be sure that all iOS devices can get access?

    A. Add a Student Portal app from the Apple App Store.

    B. Create a device enrollment manager account.

    C. Configure an Intune Service Connector for Exchange.

    D. Import an Apple Push Notification service (APNs) certificate.

5. You are the administrator for Stormwind Studios. Stormwind has subscribed to Microsoft Intune. All of your client computers are running Windows 10 Enterprise. Users are complaining that they get prompted to restart their systems after mandatory updates. You need to stop the prompts from appearing on the clients Windows 10 systems following their updates. Which Intune policy template should you use?

A. Microsoft Intune Agent Settings.

B. Windows Intune Policy Configuration.

C. Microsoft Intune Security Settings.

D. You need to create a Custom Windows 10 Policy.

6. You are the IT Manager for WillPanek.com. The company has an Active Directory domain and a cloud-based Azure Active Directory. The two are synchronized by using the Azure Active Directory Synchronization Tool. The company also uses System Center Configuration Manager. You need to use Configuration Manager to manage devices registered with Intune. What do you need to do to accomplish this? (Choose two.)

A. Create a new device enrollment manager account in Microsoft Intune.

B. In Microsoft Intune, configure an Active Directory Connector.

C. Configure the Microsoft Intune Connector role in Configuration Manager.

D. Create the Microsoft Intune subscription in Configuration Manager.

7. You are the administrator of your organization's Active Directory domain. The owners of the company want to move to the cloud by using Azure Active Directory. You need to be able to have the on-site version of Active Directory work with the cloud-based Azure Active Directory. What do you need to install to make this happen?

A. The Active Directory (AD) user connector

B. Azure Active Directory (AD) Connect tool

C. Microsoft Intune Connection tool

D. Microsoft Intune single sign-on tool

8. You are the IT director for large company that has decided to move to the cloud. The company wants to use Azure Active Directory and Microsoft Intune. The company has been looking into this because users have been using multiple devices to get their job done. When your users get added to Intune and get licensed, how many devices can each user add by default?

A. 3

B. 4

C. 5

D. None. Device Administrators are the only person who can add devices to Intune.

9. You are the administrator of a company that builds its own applications. You have decided that you want to install a company application to all employees by using the Windows Store. Which term is used to refer to installing corporate apps through the Windows Store?

A. WS Installations

B. BranchCache

    C. Image installation

    D. Sideloading

10. You are the IT Director for Stormwind training studios. Your company has decided to start using Microsoft Intune for all of their software deployments. You want to set up a notification system so that you see all alerts and that you IT Manager only gets notified for Critical alerts. How do you accomplish this? (Choose all that apply.)

    A. Set up all event notifications for the IT Manager in Intune.

    B. Set up all event notifications for the IT Director in Intune.

    C. Set up Critical event notifications for the IT Manager in Intune.

    D. Set up Critical event notifications for the IT Manager in Intune.

Chapter

7

Configuring Applications

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Deploy and manage Azure RemoteApp.**

- This objective may include but is not limited to the following subobjectives: Configure RemoteApp and Desktop Connections settings, configure Group Policy Objects (GPOs) for signed packages, subscribe to the Azure RemoteApp and Desktop Connections feeds, export and import Azure RemoteApp configurations, support iOS and Android, configure remote desktop web access for Azure RemoteApp distribution.

✓ **Support desktop apps.**

- This objective may include but is not limited to the following subobjectives: The following support considerations including: Desktop app compatibility using Application Compatibility Toolkit (ACT) including shims and compatibility database; desktop application co-existence using Hyper-V, Azure RemoteApp, and App-V; installation and configuration of User Experience Virtualization (UE-V).

✓ **Support Windows Store and cloud apps.**

- This objective may include but is not limited to the following subobjectives: Install and manage software by using Microsoft Office 365 and Windows Store apps, sideload apps into online and offline images, integrate Microsoft account including personalization settings.

In this chapter, we will look at how to configure applications on Windows 10. One of the issues with applications is that they may not work properly on a newer operating system. We will look at the ways to allow older applications to work on Windows 10.

We will also look at two different ways to browse the Internet: Edge and Internet Explorer. As the Internet and the World Wide Web have increased exponentially in both content and features, Microsoft has continually enhanced and added new functionality to its browser. The current version is Windows Internet Explorer 11, or IE11.

With the increase in the functionality of browsers and in their ease of use, there has been an increase in the way websites are used to provide content for end users in the public space (Internet browsing) as well as for private corporate browsing. With the introduction of IE11, Microsoft has taken the usability that end users want to new levels as well as provided a good deal of security enhancement. This gives the user the best and easiest browsing environment and provides a balance of security information about the sites and pages being viewed.

Supporting Desktop Applications

As IT professionals, many of us think of managing applications simply as installing applications on the computer. But there are other details that may need to be configured to allow applications to run faster and more efficiently.

As operating systems evolve, one issue that you can run into is that your applications may not work properly on the newer version of the operating system. Microsoft has developed a few different ways to help you combat this issue.

Using the Application Compatibility Toolkit (ACT)

When new Windows operating systems are installed, applications that ran on the previous version of Windows may not work properly. The Application Compatibility Toolkit (ACT) allows an administrator to help solve these issues before they occur.

The Application Compatibility Toolkit allows IT professionals to decide if an application is compatible with the Windows 10 operating system before rolling out the new Windows 10 OS to the entire network. ACT also allows IT departments to decide how updating to Windows 10 will impact the applications on the domain.

IT professionals can use the ACT features to do the following:

- Verify that all of the corporate applications and computer hardware are compatible with Windows 10.
- Test the corporate applications for User Account Control (UAC)–related issues.
- Test the corporate web applications and websites for compatibility with new versions and security updates to Windows Internet Explorer.

After installing ACT, there are three phases of how ACT works within the network.

Phase 1: Collecting Your Compatibility Data   Phase 1 consists of your IT department collecting all compatibility data from the software packages as well as creating and configuring your data-collection packages (DCPs). Phase 1 also includes information about how to distribute your DCPs and how to perform common collection tasks, such as importing or exporting DCP settings.

Phase 2: Analyzing Your Compatibility Data   Phase 2 analyzes the information that you collected in Phase 1. Phase 2 allows an administrator to gather information and procedures and to filter and organize the data collected in Phase 1. Phase 2 also provides information about your application compatibility reports, issues, and solutions.

Phase 3: Testing and Mitigating Your Compatibility Issues   Phase 3 consist of testing guidance and procedures for using the development tools. These tools include the Standard User Analyzer (SUA), the Internet Explorer Compatibility Test Tool (IECTT), and the Compatibility Administrator, which allow administrators to fix their compatibility issues. Phase 3 also consists of information about the application fix (also known as "Shims") library, and the known Internet Explorer security feature issues.

Understanding Application Fix (Shims)

When new operating systems get released, older applications may not run, and you may not be able to get a newer version of the application. For example, a vendor that sold you an application may have gone out of business, but the application is still needed in your organization.

If you install the application on Windows 10, there may be issues. This is where Shims will apply. The *Shims* is a coding fix that allows the application to function properly.

The Shim Infrastructure consists of application programming interface (API) hooking. This means the Shim Infrastructure uses linking to redirect API calls from the Windows operating system to the alternative code called the shim.

To have Shims created, you must first contact Microsoft. Microsoft must create the Shim; Microsoft does not offer any custom tools to allow for private creation. Microsoft does include shims with Windows 10, and new shims will be available through Windows Update as they are created.

File Extension Association

When dealing with applications and software packages, you may need to associate a file extension (shown in Figure 7.1) with a software package. For example, you may want all

files with the filename extension .asx to be played through Windows Media Player. You have the ability to set these file-extension associations in Default Programs in Control Panel. Within Default Programs, there is link called "Associate a file type or protocol with a specific program."

FIGURE 7.1   Filename-extension association
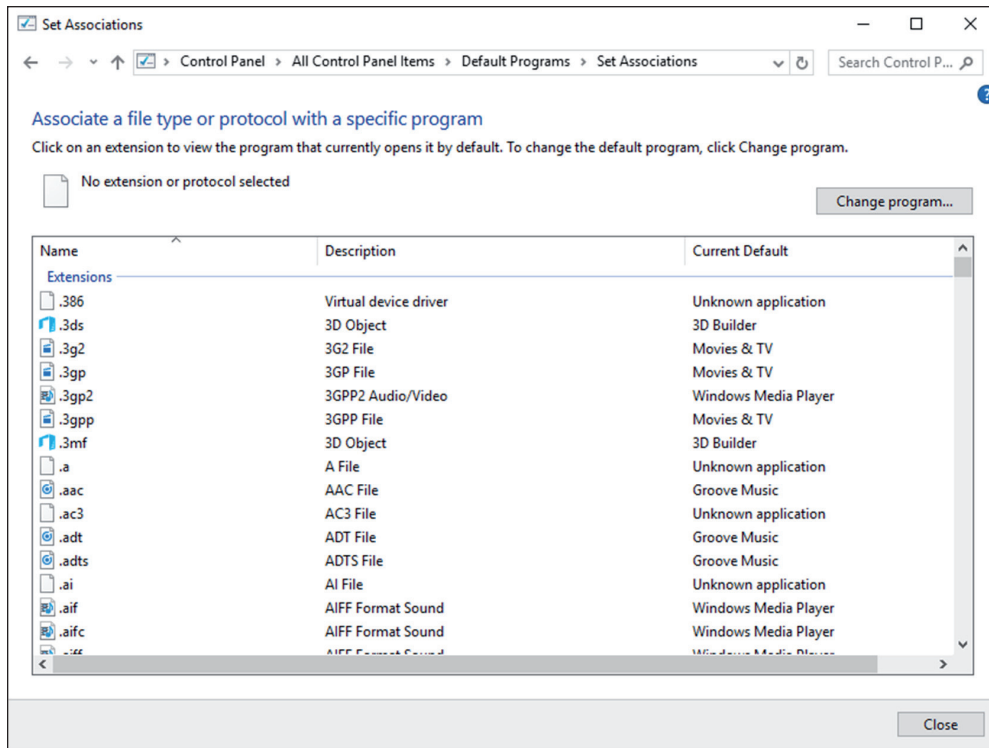
Using Hyper-V for Desktop Applications

Virtualization—the ability to run one operating system on top of another—is sweeping the computer industry. Microsoft has a virtualization environment called *Hyper-V* that can operate on its client software. Hyper-V allows you to create and manage virtual machines without the need for a server operating system on different hardware. The advantage of virtualization is that you can run multiple operating systems like Windows XP, Windows Vista, Windows 7, Windows 8/8.1, or Windows 10 all on the same hardware.

Hyper-V gives you the ability to set up virtualization on a client operating system. This is very beneficial for anyone in the industry who has to do testing or configuration. Hyper-V on Windows 10 is not really meant to run a network as Hyper-V on Windows Server 2012 R2 does, but it does give an administrator the ability to test software and patches before

installing them live on a network or running applications in an operating system other than the installed one. Also, it is beneficial to research problems in a controlled environment and not on a live system where you can end up doing more harm than good.

Finally, Hyper-V gives you a training advantage. Think about having the ability to train users on a real product like Windows Server 2012 R2 or Windows 10 without needing to purchase additional equipment. Hyper-V allows you to train users on products and software while using only one machine. I will now briefly explain the differences between these forms of virtualization:

Server Virtualization   This basically enables multiple servers to run on the same physical server. Hyper-V is a server virtualization tool that allows you to move physical machines to virtual machines and manage them on a few physical servers. Thus, you will be able to consolidate physical servers.

Presentation Virtualization   When you use *presentation virtualization*, your applications run on a different computer and only the screen information is transferred to your computer. An example of presentation virtualization is Microsoft Remote Desktop Services in Windows Server 2012 R2.

Desktop Virtualization   *Desktop virtualization* provides you with a virtual machine on your desktop, comparable to server virtualization. You run your complete operating system and applications in a virtual machine so that your local physical machine just needs to run a very basic operating system. An example of this form of virtualization is Microsoft Virtual PC.

Application Virtualization   *Application virtualization* helps prevent conflicts between applications on the same PC. Thus, it helps you to isolate the application running environment from the operating system installation requirements by creating application-specific copies of all shared resources, and it helps reduce application-to-application incompatibility and testing needs. An example of an application virtualization tool is Microsoft Application Virtualization (App-V).

🌐 Real World Scenario

Hyper-V Advantages

As an instructor and consultant, I can't say enough about how valuable Hyper-V can be as a tool. I have used it on many occasions to either test a piece of software before installation or find an answer to a problem in a controlled environment.

At the time this book is being written, I use Microsoft Windows 7 Professional on my laptop. On that same laptop I have a version of virtualization with both Windows Server 2012 R2 and Windows 10 Professional operating system virtual machines.

While I am on a client site or while I am in the classroom, having a way to test and research problems using multiple operating systems on one client computer system is invaluable.

Hyper-V Features

As a lead-in to the virtualization topic and Hyper-V, I will start with a list of key features, followed by a list of supported guest operating systems. This should provide you with a quick, high-level view of this feature before we dig deeper into the technology.

Key Features of Hyper-V

The following list briefly describes the key features of Hyper-V:

New Architecture   The hypervisor-based architecture, which has a 64-bit micro-kernel, provides an array of device support as well as performance and security improvements.

Operating System Support   Both 32-bit and 64-bit operating systems can run simultaneously in Hyper-V. Also, different platforms like Windows, Linux, and others are supported.

Support for Symmetric Multiprocessors   Support for up to four processors in a virtual machine environment provides you with the ability to run applications as well as multiple virtual machines faster.

Network Load Balancing   Hyper-V provides support for *Windows Network Load Balancing (NLB)* to balance the network load across virtual machines on different servers.

New Hardware Architecture   Hyper-V's architecture provides improved utilization of resources like networking and disks. This allows an IT department the ability to run multiple operating systems on the same host without each system interfering with the other systems.

Quick Migration   Hyper-V's *Quick Migration* feature provides you with the functionality to run virtual machines in a clustered environment with switchover capabilities when there is a failure. Thus, you can reduce downtime and achieve higher availability of your virtual machines.

Virtual Machine Snapshot   You can take snapshots of running virtual machines, which provides you with the capability to recover to any previous virtual machine snapshot state quickly and easily.

Resource Metering   Hyper-V *resource metering* allows an organization to track usage within the businesses departments. It allows an organization to create a usage-based billing solution that adjusts to the provider's business model and strategy.

Scripting   Using the Windows Management Instrumentation (WMI) interfaces and APIs, you can easily build custom scripts to automate processes in your virtual machines. Administrators also have the ability to use PowerShell cmdlets to do scripting.

RemoteFX   Windows 10 Hyper-V RemoteFX allows for an enhanced user experience for RemoteFX desktops by providing a 3D virtual adapter, intelligent codecs, and the ability to redirect USB devices in virtual machines.

Fibre Channel   The virtual Fibre Channel feature allows you to connect to the Fibre Channel storage unit from within the virtual machine. *Virtual Fibre Channel* allows an administrator to use their existing Fibre Channel to support virtualized workloads. Hyper-V users have the ability to use Fibre Channel storage area networks (SANs) to virtualize the workloads that require direct access to SAN logical unit numbers (LUNs).

Enhanced Session Mode   Enhanced Session Mode enhances the interactive session of the Virtual Machine Connection for Hyper-V administrators who want to connect to their virtual machines. It gives administrators the same functionality as a remote desktop connection when the administrator is interacting with a virtual machine.

In previous versions of Hyper-V, the virtual machine connection gave you limited functionality while you connected to the virtual machine screen, keyboard, and mouse. An administrator could use an RDP connection to get full redirection abilities, but that would require a network connection to the virtual machine host.

Enhanced Session Mode gives administrators the following benefits for local resource redirection:

- Display configuration
- Audio
- Printers
- Clipboard
- Smart cards
- Drives
- USB devices
- Supported Plug and Play devices

Shared Virtual Hard Disk   Windows 10 Hyper-V has a feature called Shared Virtual Hard Disk; Shared Virtual Hard Disk allows an administrator to cluster virtual machines together by using the shared virtual hard disk (VHDX) files.

Shared virtual hard disk allows an administrator to build a high availability infrastructure which is very important if you are setting up either a private cloud deployment or a cloud-hosted environment for managing large workloads. Shared virtual hard disks allow two or more virtual machines to access the same virtual hard disk (VHDX) file.

Automatic Virtual Machine Activation (AVMA)   Automatic Virtual Machine Activation (AVMA) is a new feature that allows administrators to install virtual machines on a properly activated Windows 10 system without the need to manage individual product keys for each virtual machine. When using AVMA, virtual machines get bound to the licensed Hyper-V server as soon as the virtual machine starts.

Dynamic Memory   *Dynamic Memory* is a new feature of Hyper-V that allows it to balance memory automatically among running virtual machines. Dynamic Memory allows Hyper-V to adjust the amount of memory available to the virtual machines in response to the needs of the virtual machine. It is currently available for Hyper-V in Windows 10.

Installing Hyper-V

To run Hyper-V, you need a minimum processor of an x64-compatible processor with Intel VT or AMD-V technology enabled. Hardware Data Execution Prevention (DEP), specifically Intel XD bit (execute disable bit) or AMD NX bit (no execute bit), must be available and enabled. Minimum: 1.4 GHz. Recommended: 2 GHz or faster.

Your system memory (RAM) should be at minimum at least 1 GB of RAM, but recommended is at least 2 GB RAM or greater (additional RAM is required for each running guest operating system) with a maximum of 1 TB.

Your system's hard drive should be a minimum of 8 GB, recommended 20 GB or greater. (Additional disk space needed for each guest operating system.).

You can load Hyper-V on some versions of the following operating systems: Windows 10, Windows 8/8.1, and Windows Server 2008/2008 R2 and 2012/2012 R2. As for as Windows 10 Hyper-V, you need to use one of the following versions: Enterprise, Professional, or Education. Exercise 7.1 walks you through the process of installing the Hyper-V role on Windows 10 Enterprise.

EXERCISE 7.1

Installing Hyper-V

1. Open the Programs And Features tool by clicking Start ➤ Control Panel ➤ Programs And Features.

2. Click the Turn Windows Features On Or Off link in the upper-left corner.

3. Scroll down the features list and check the Hyper-V check box (shown in Figure 7.2). Click Next.

FIGURE 7.2 Hyper-V check box
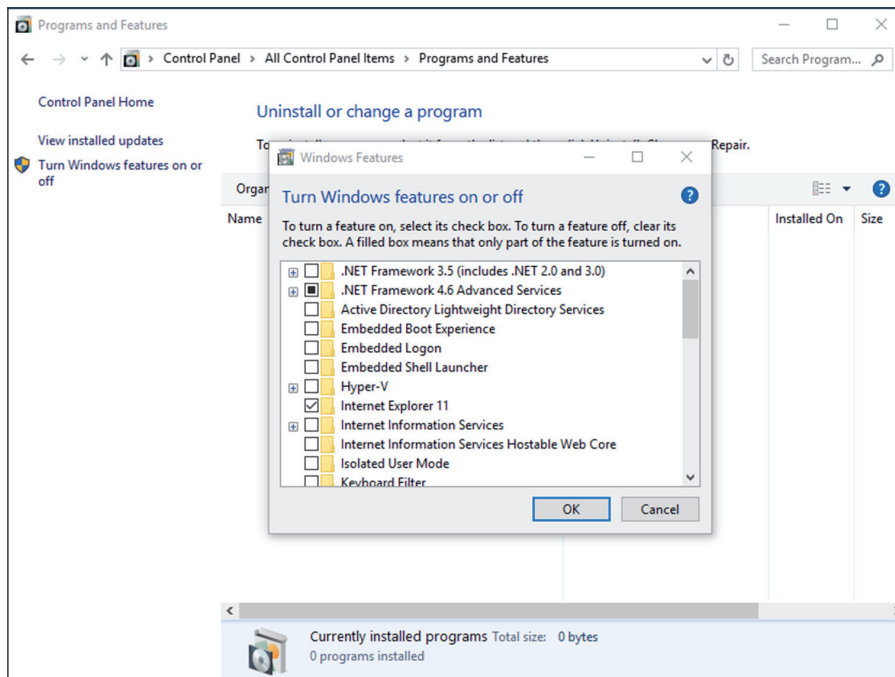
4. The installation wizard will take a few minutes to install Hyper-V. Once Windows has finished installing Hyper-V, click the Close button.

5. Restart your server.

> **NOTE** There may be a time when you need to remotely execute PowerShell commands on a virtual machine. To do this, you need to run the `Invoke-Command` command and specify which VM you're connecting to (the `-VMName` parameter).

Configuring User Experience Virtualization (UE-V)

To help you fully understand the benefits of Microsoft User Experience Virtualization (UE-V), I need to explain the benefits of roaming profiles. Roaming profiles were used to allow a user to go from one system to another but still have the exact same desktop and settings. Well UE-V is roaming profiles on steroids.

Microsoft UE-V is a virtualization platform that allows users to move from one Windows system to another but they get to keep the same Windows operating system and all of their settings. This allows users to feel comfortable moving from one device to another because their current operating system and settings follow them wherever they go.

So how does UE-V actually allow users to move around? UE-V uses XML templates that allow users to save their operating system and settings. Actually, with the use of the XML template files, you can choose which settings get saved and moved between Windows operating systems. The XML templates know exactly how all of the application settings are saved throughout the file system.

Microsoft UE-V provides the following benefits:

- Administrators have the ability to specify exactly which application and desktop settings synchronize between the operating systems.

- Administrator have the ability to create their own custom templates for third-party applications.

- Users have the ability to recover their settings and applications after any type of hardware changes.

- Users can access their settings from any location and on any Windows device.

UE-V Components

Now that you understand UE-V, let's take a look at some of the components needed to make it all work properly. Table 7.1 lists all of the different components and describes what each component does.

TABLE 7.1   UE-V components

Component	Description
UE-V agent	The UE-V agent gets installed on every Windows operating system that you want to synchronize settings with. The UE-V agent also observes all of the applications and settings for the Windows operating system.
Settings packages	UE-V agents take all of the settings and applications on a system and turn those into an application package. These application packages are created locally, and then they are copied to a shared network location.
Settings storage share	Administrators must create a network share that will house all of the setting packages. The UE-V agent will verify that the network share is configured properly, and then the UE-V agent will create a hidden system folder for the user's settings.
Settings location templates	XML templates are used to synchronize the application and settings files. UE-V includes a few templates by default, but you have the ability to create your own.
Windows apps list	The Windows apps list is used to determine which Windows applications will get synchronized. UE-V uses the Windows apps list to know which apps and files get copied to the settings package.

Installing and Configuring UE-V

Installing UE-V is not a very complicated process. First thing that you must do is download the Microsoft Desktop Optimization Pack (MDOP). Microsoft UE-V is part of the MDOP software package. Then you need to create a network share that we can store your UE-V templates at. After the share is created, you must make sure that you set up the permissions properly on that shared drive. After you have created the network share, you then have to install the UE-V agent. The UE-V agent allows the Windows operating system to share its settings to the network. Then you just need to test your configurations, and you are all set. To set up the UE-V agent, you need to run the following executable along with the path of the network share:

```
AgentSetup.exe SettingsStoragePath=\\server\settingsshare\%username%
```

When you install UE-V, certain Windows files and apps get stored automatically. The following list shows some of the apps and files that get copied automatically.

UE-V synchronizes settings for some Microsoft applications by default. Here is a partial list of just some of the applications that get synchronized by default:

▪   Microsoft Office 2013 applications (UE-V 2.1 SP1 and 2.1)

▪   Microsoft Office 2010 applications (UE-V 2.1 SP1, 2.1, and 2.0)

- Microsoft Office 2007 applications (UE-V 2.0 only)
- Internet Explorer 8, 9, and 10
- Internet Explorer 11 in UE-V 2.1 SP1 and 2.1
- Windows applications, such as Xbox
- Windows desktop applications, such as Microsoft Calculator, Notepad, and WordPad
- Windows settings, such as desktop background or wallpaper

> Since the Microsoft Desktop Optimization Pack is needed to do this installation, I did not include a lab. If you have the ability to download the MDOP, go to `https://technet.microsoft.com/en-us/library/dn479305(v=vs.85)` `.aspx` to get step-by-step procedures for installing and using UE-V.

Understanding AppLocker

Since we're talking about how we should support applications, then we also need to look at how we lock down applications. AppLocker is a feature included with Windows (Windows 7 and higher) that allows administrators to lock out certain applications from running. AppLocker can also be run from a GPO on a Windows Server (2008 and above) to lock an application out of the entire domain.

AppLocker allows administrators to control how network users can access and use certain files like executables (`.exe` and `.com`), scripts (`.ps1`, `.bat`, `.cmd`, `.vbs`, and `.js`), DLLs (`.dll` and `.ocx`), and Windows Installer files (`.msi` and `.msp`). AppLocker allows you to do the following;

- Test the AppLocker policy before implementing it by using the audit-only mode.
- Set file attribute rules using the application's digital signature, product name, filename, or even file version.
- Place rules on individuals or security groups.
- Set exceptions for any rule.
- Administrators have the ability to import or export rules.
- AppLocker can be managed by using PowerShell cmdlets.

When setting an AppLocker rule, all files for that rule will be denied from working unless you create a rule exemption. If there are no AppLocker rules for a specific file format, then all of those files will be allowed to work on the system. When setting AppLocker rules, the rules can be allowed or denied.

Allow: Administrators have the ability to determine which files are permitted to run in the corporate environment. Administrators also have the ability to configure exceptions to the rules.

Deny: Administrators have the ability to determine which files are *not* permitted to run in the corporate environment. Administrators also have the ability to configure exceptions to the rules.

Understanding Azure

Before I start talking about Azure, you first must understand that Azure is more than one thing—it's like a suite of tools and applications. Azure is a subscription-based service from Microsoft that offers many resources to help any size organization get the most out of Microsoft products. Figure 7.3 shows just some of the services offered by Azure. You have the ability to use Azure Active Directory, Azure backups, Windows applications, Azure virtual machines, and Windows Servers, among many other things.

FIGURE 7.3   Azure options
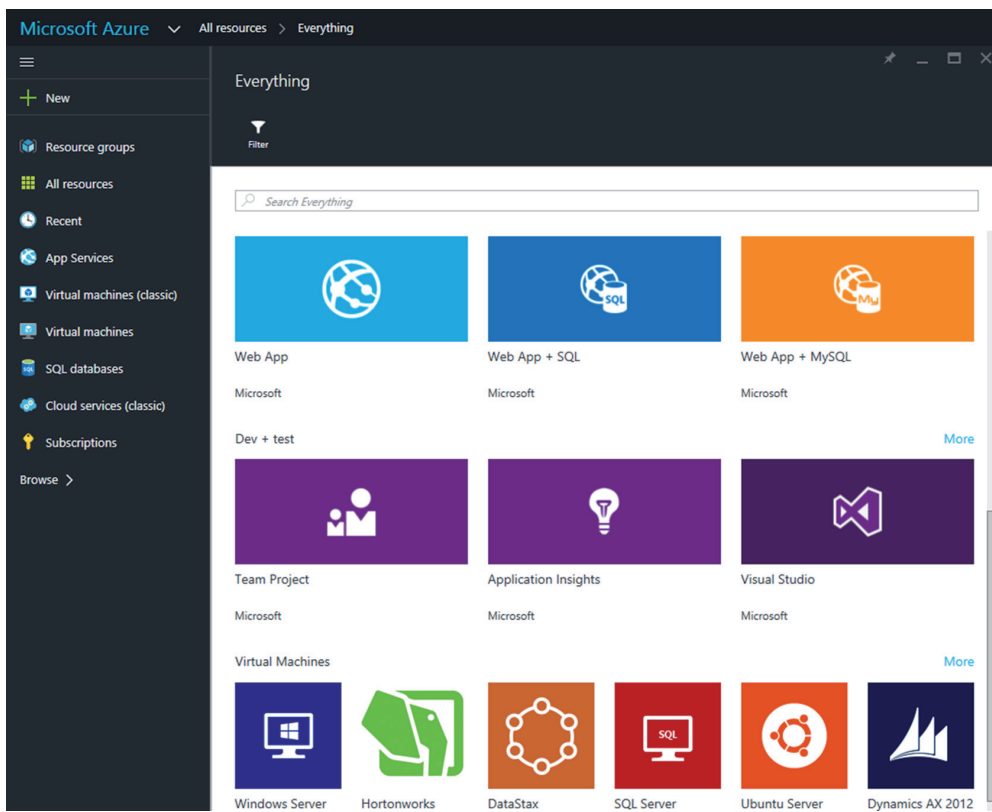
Azure Active Directory is the Microsoft version of Directory Services. In short, Active Directory is a set of services that help you secure and manage your network. There are multiple components of Active Directory:

▪   Active Directory Domain Services (AD DS)

▪   Active Directory Certificate Services (AD CS)

- Active Directory Federation Services (AD FS)
- Active Directory Rights Management Services (AD RMS)
- Active Directory Lightweight Directory Services (AD LDS)

> **NOTE** I will talk about Active Directory in greater detail in Chapter 9, "Configuring Network Connectivity."

Let's look at some of the Azure applications (some of which are shown in Figure 7.4) that you can configure and manage, starting with All Items in the upper-left corner.

FIGURE 7.4   Azure applications
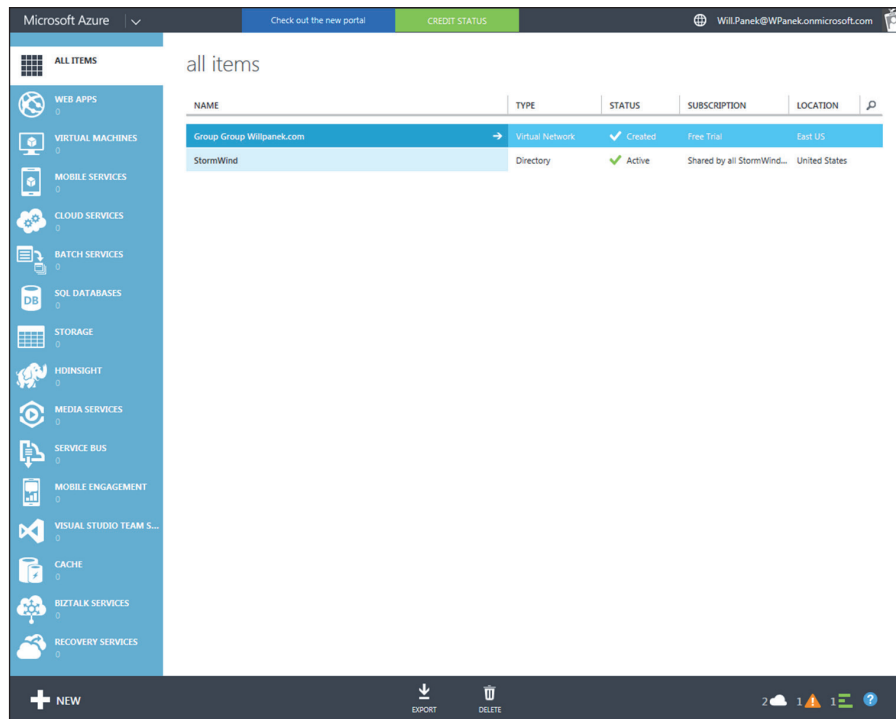
All Items   The All Items feature shows you all of the applications and services that you currently subscribe to. The All Items feature allows you to manage and manipulate all of your services from one location.

Web Apps   The Web Apps feature allows developers to quickly develop, deploy, and manage websites and web apps. Developers can build web apps using .NET, Node.js, PHP, Python, and Java. Developers can use a single backend to create web apps and mobile apps for employees or customers.

Virtual Machines   The Virtual Machine feature allows IT Administrators to quickly create and manage cloud-based virtual machines. The Virtual Machines feature allows an administrator to quickly deploy a wide range of computing solutions and pay by the minute for the use of the virtual machines. The Virtual Machine Feature allows an administrator to work with multiple operating systems including Windows, Linux, Microsoft SQL Server, Oracle, IBM, SAP, and Azure BizTalk Services.

Cloud Services   Azure Cloud Services allows an organization to create, package, and deploy applications and services to the cloud with the click of a button. Once an organization creates an application, Microsoft does the rest. Azure handles all aspects from provisioning, load-balancing, and health monitoring. Your organization's application is supported by an industry-leading 99.95-percent guaranteed uptime.

Batch Services   Azure Batch services allow you to execute large-scale batch jobs. Administrators have the ability to run these batch jobs either on demand or on a schedule.

SQL Databases   Azure SQL Database is a database service modeled after the Microsoft SQL Server software. The one major advantage of using the cloud-based version of SQL services is that you get all of the benefits of SQL like performance, scalability, no downtime, business continuity, and data protection—all with near-zero administration. This gives your organization the ability to focus on application development instead of focusing on managing virtual machines and infrastructure. The SQL Database feature is available in Basic, Standard, and Premium service tiers.

Storage   Azure Storage provides organizations with the ability to store and retrieve large amounts of data in the cloud. Administrators have the ability to store data, such as documents and media files, while giving your organization scalability, reliability, and redundancy. Through the use of Microsoft's Azure cloud-based system, you get a cost-efficient way to store all of your company's data in one location.

HDInsight   Azure HDInsight is an Apache Hadoop server located in the cloud. Using HDInsight allows an organization to handle any amount of data on demand, from gigabytes to petabytes.

Media Services   Azure Media Services gives a company the ability to enable enterprise streaming solutions worldwide. Azure Media Services allows a company to have a powerful and scalable cloud-based encoding, encryption, and streaming system.

Service Bus   Azure Service Bus is a cloud-based messaging system for connecting applications, services, and devices. The real advantage of using Azure Service Bus is that you can connect any of these items wherever the items are located. You can even use Service Bus to connect other devices like tablets or phones to an application or each other.

Mobile Engagement   The Mobile Engagement feature gives an organization the ability to have real-time analytics. Using these analytics allows an IT department to solve problems with their network or applications. For example, you can see if your network is having bottlenecks and take measure to help solve the bottleneck.

Visual Studio Team Services   Visual Studio is one of the most popular ways for developers to create packages. Visual Studio Team Services allows developers to plan, build, and send software across a multitude of operating systems. Since this is a cloud-based app, the advantage of using Visual Studio Team Services is that you get the benefits of Visual Studio without having the need to install or configure a single Windows server.

Cache   Microsoft Azure Cache allows quick access to your corporate applications without the need to have a lot of memory local on your system. The Cache is a cloud-based memory system that is a scalable solution that allows corporations to create applications by providing fast access to data.

BizTalk Services   BizTalk Services allows cloud-based applications to communicate with each other or with on-premise applications. Because cloud-based apps run in their own cloud space, there is an issue with messaging and transport protocol mismatches. This is where BizTalk can help. BizTalk bridges the gap between the apps and your onsite services.

Recovery Services   Azure Recovery Services allows an organization to back up and recover their data in the cloud. Recovery Services is a subscription-based backup service that is controlled by Microsoft.

Scheduler   Azure Scheduler allows an administrator to schedule jobs in the cloud that consistently initiate service requests inside or outside of Azure. Administrators have the ability to run tasks right away, on a recurring schedule, or in the future.

API Management   Microsoft Azure API (application program interface) Management allows an administrator to manage APIs among internal departments, partners, and developers. API Management allows administrators to use the tools needed for provisioning user roles, developing usage plans and quotas, applying policies, and monitoring alerts.

Networks   Azure Virtual Network allows you to create an isolated and secure environment that you can run virtual machines and applications in. Administrators can use private IP addresses, subnets, access control policies, and almost anything that you can do with a physical network.

RemoteApp   Azure RemoteApp allows an administrator to provide secure, remote access to applications from multiple user devices. Azure RemoteApp allows users to host temporary Terminal Server sessions in the cloud. These Terminal Server sessions can be used and shared by other users in your network. RemoteApp is discussed in greater detail in the "Using Azure RemoteApp and App-V" section that follows this list of apps.

Active Directory   Azure Active Directory allows an organization to use and manage an Active Directory network without the need of setting up Windows Servers. Users can still use a single sign-on for any cloud-based or web application.

Marketplace   Azure Marketplace is your one-stop store for thousands of software applications, developer services, and data. These applications are automatically configured for use with Microsoft Azure.

Using Azure RemoteApp

As stated earlier in the chapter, Azure RemoteApp allows an administrator to provide secure, remote access to applications from multiple user devices. Azure RemoteApp allows users to host temporary Terminal Server sessions in the cloud. These Terminal Server sessions can be used and shared by other users in your network.

Azure RemoteApp allows users to share resources and applications on any device type. It can do this because your organization's applications are hosted in the cloud. Since all of your applications are cloud-based, any device with Internet access can then gain access to the applications. The one main advantage of using Azure RemoteApp is that you do not need to build and use servers in your organization to run your apps. After you upload your applications to the cloud, you then manage all of your applications through the Azure portal.

Then after the applications are loaded to the cloud, your users can access those applications from any device in the world. It does not matter on the application. Any application that is loaded to the cloud can then be accessed from the cloud. Users will need to download the Azure RemoteApp client to have web access for Azure RemoteApp.

> **NOTE**   If you want your users to have web access to Azure RemoteApp, you need to download a RemoteApp client on your device. To do this, go to `https://www.remoteapp.windowsazure.com/en/clients.aspx`.

Since the applications are loaded onto virtual machines, the applications can be accessed by any type of device, including Apple devices and Android devices. Azure RemoteApp even supports application streaming for both 32-bit and 64-bit applications as long as they are loaded onto a Windows Server 2012 R2 virtual machine.

Creating Collections in Azure RemoteApp

The first thing you need to do to Azure RemoteApp is set up your application collections. Collections are just storage containers for applications and users. Every software image gets its own collection in the cloud.

Let's take a look at how to create an Office 2013 collection. Exercise 7.2 walks you through the creation of a collection for Office 2013.

EXERCISE 7.2

Creating a Collection

1. Open the Azure portal.

2. In the tree on the left, scroll down until you see RemoteApp. Click the RemoteApp feature (shown in Figure 7.5).

   FIGURE 7.5   RemoteApp feature
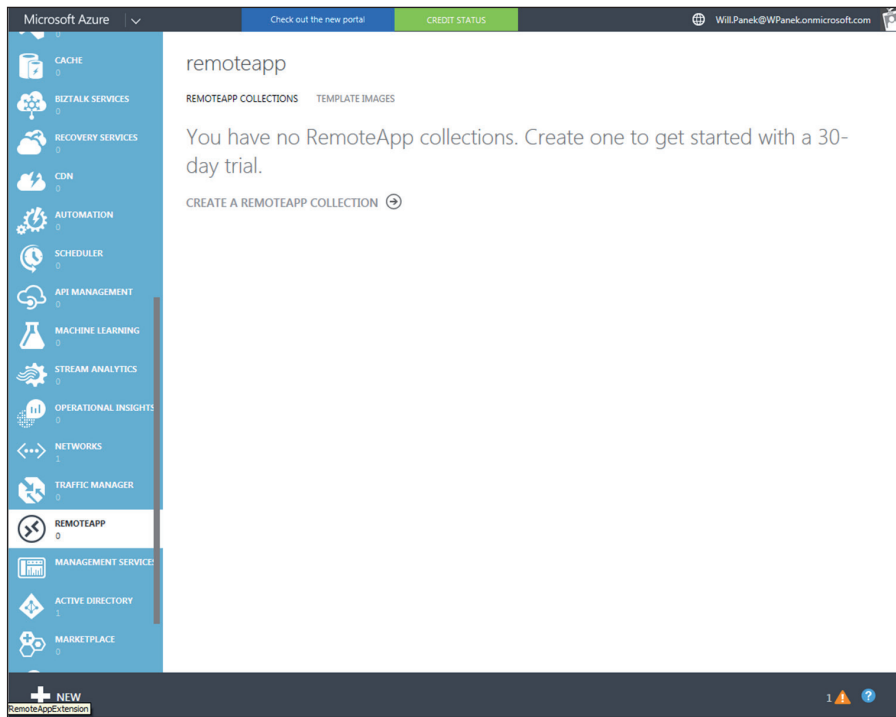
3. Click the Create a RemoteApp Collection link.

4. Click the Quick Create option and then enter a name for your collection (see Figure 7.6).

5. Select your region. If your region is not listed, choose the closest region to your own.

6. Select the billing plan you want to use. For this exercise, select the Basic package.

7. Finally, select the Office 2013 Professional image. This image contains Office 2013 apps. This image is good only for trial collections. You can't use this image in a production environment.

8. Click the Create RemoteApp Collection link.

FIGURE 7.6 Quick Create option
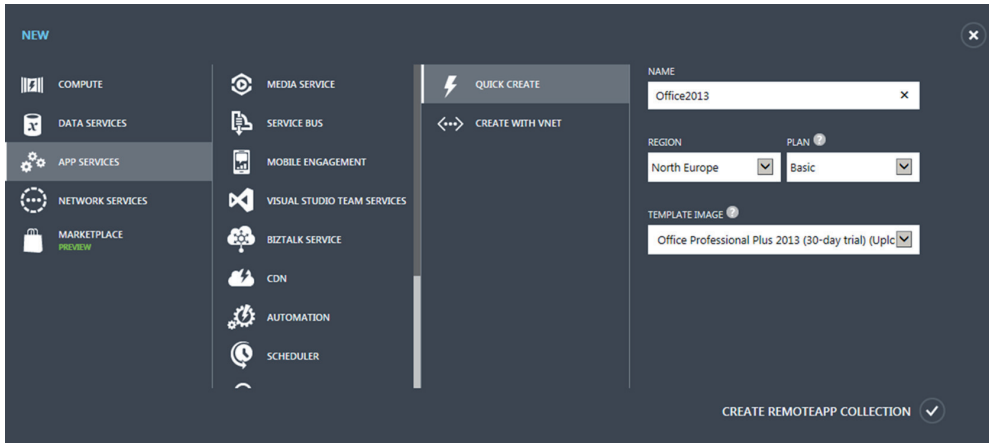
Sharing an Application

Now that you have created a collection, you have to share the application so that users can gain access. To share the application, follow the steps in Exercise 7.3.

E X E R C I S E 7.3

Sharing the Collection

1. Open the Azure portal.

2. In the tree on the left, scroll down until you see RemoteApp. Click the RemoteApp feature.

3. Click the arrow to the right of the collection name that you created in Exercise 7.2.

4. Click the Publishing tab on the top. Click Publish at the bottom of the screen, and then click Publish Start Menu Programs.

5. Next, you need to select the apps that you want to publish. For this exercise, I chose Word. Click Complete. You will then need to wait for the application to complete its publishing.

6. Once the application has completed publishing, click the User Access tab to add the users who will require access to the application. Enter each user's email address and then click Save.

Setting Up RemoteApp Connection Feeds

One of the issues that previous versions of RemoteApp encountered was that the applications ran in a web page and needed to be started from a web location. With Windows Server 2008 R2 and 2012/2012 R2 and Windows 7/8/8.1/10, you can now add the program to the users' Start menu. This gives your users the same program startup as if they had the program installed on their machine.

RemoteApp along with Desktop Connections allow for a feature called RemoteApp and Desktop Connection Feed. When using RemoteApp and Desktop Connection Feed, your users will subscribe to a RemoteApp programs feed (a URL). Once your clients subscribe to the feed, the application will be displayed on the users' Start menu.

To set up the RemoteApp and Desktop Connection feed, you need to create a new feed in Control Panel. To complete these steps, you will need to get the URL of the feed. To do this, go into the Azure Portal ➤ RemoteApp and then click the collection you created. There will be a URL link that you can use for the feed. You have to create a published feed on a virtual machine to get a proper URL and then use that link for setting up the feed. The following steps walk you through how you would set up a feed on a Windows 10 machine:

1. Open RemoteApp And Desktop Connections in Control Panel (shown in Figure 7.7).

FIGURE 7.7 RemoteApp And Desktop Connections
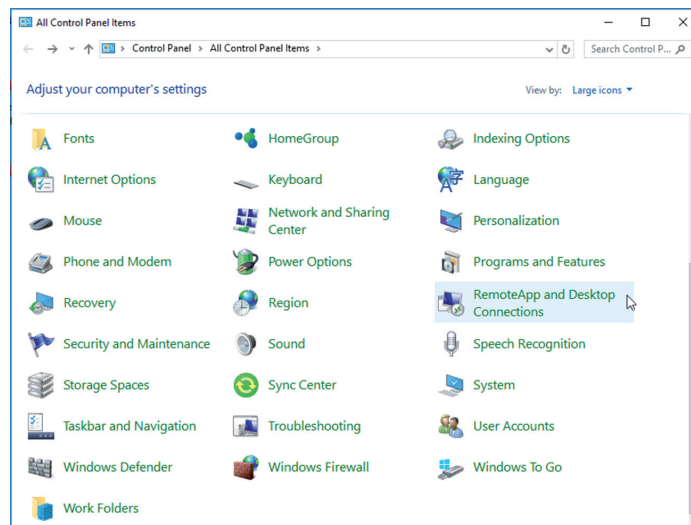
2. Click the Access RemoteApp And Desktops link on the left side of the screen.

3. Enter the URL of the collection feed and click Next.

4. On the Ready To Setup The Connection screen, click Next.

5. On the sign-in screen, enter your credentials. Click OK.

6. On the Summary screen, click the Finish button.

7. Start the application by accessing your system's Start menu.

Using Device Redirection

RemoteApp device redirection allows an administrator to configure a Windows system so that your users' devices can interact with the remote applications. For example, if you want to set up Skype through RemoteApp, a user would still need his or her camera and microphone to work with the RemoteApp version of Skype.

Administrators have the ability to set up RemoteApp device redirection through the use of a GPO, or they can set up the collection to automatically use redirection. To set up the collection for redirection, you would need to run some PowerShell commands. Table 7.2 lists some of the PowerShell commands and describes what they do.

TABLE 7.2 RemoteApp PowerShell commands

PowerShell Command	Description
Set-AzureRemoteAppCollection -CollectionName <collection name> -CustomRdpProperty "drivestoredirect: s:*'nusbdevicestoredirect:s:*"	This command sets the custom RDP properties.
Get-AzureRemoteAppCollection -CollectionName <collection name>	This command shows you a list of what custom RDP properties are configured.
Set-AzureRemoteAppCollection -CollectionName <collection name> -CustomRdpProperty "drivestoredirect:s:*"	This command shows you how to set up hard-drive redirection.
Set-AzureRemoteAppCollection -CollectionName <collection name> -CustomRdpProperty "drivestoredirect: s:*'nusbdevicestoredirect:s:*"	This command shows you how to set up USB and hard-drive redirection.
Install-Module AzureRM Install-AzureRM	These commands allow you to install the Azure Resource Manager modules.
Install-Module Azure	This command installs the Azure Service Management module.
Import-AzureRM	This command imports AzureRM modules.
Import-Module Azure	This command imports the Azure Service Management module.
Set-Mailbox	This command allows you to manipulate an Office 365 mailbox.

To configure RemoteApp redirection by using a Group Policy Object, you would complete the following steps:

> **NOTE**
> For this example, I am showing you how to configure USB redirection on a system. I am showing you how to set up a local Group Policy in the event that you do not have a Windows Server setup. If you do want to do this for a domain, create a new GPO in the Group Policy Management MMC and then follow these steps.

1. Open the Local Group Policy Editor by typing **`gpedit.msc`** into the Windows 10 Search window.
2. Expand Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\RemoteFX USB Device Redirection.
3. Double-click the "Allow RDP redirection of other supported RemoteFX USB devices from this computer" option.
4. Select Enabled, and then choose Administrators And Users in the RemoteFX USB Redirection Access Rights.
5. Close the Group Policy Editor.
6. Restart the computer.

Understanding Shared Computer Activation

There may be a time when you need to set up Office 365 ProPlus to multiple users on the same computer within your organization. To do this, you must set up shared computer activation (SharedComputerLicensing value).

Shared computer activation allows an administrator to set up Office 365 ProPlus on a single computer for multiple users. This can be useful for schools, hospitals, and hotels. Let's say that you have multiple hotel front-desk staff members who need to access data on the same remote server—this is where shared computer activation can help.

Shared computer activation is used only when you have multiple people using the same computer. If you have users in your network that each has his or her own system, you would not use shared computer activation; you would use product key activation for Office 365 ProPlus.

> **NOTE**
> To set up shared computer activation, you must use the Office Deployment Tool. For information about setting up shared computer activation, visit the Microsoft website https://technet.microsoft.com/en-us/library/dn782860.aspx?f=255&MSPPError=-2147217396.

Understanding App-V

Microsoft Application Virtualization (App-V) is included with the Microsoft Desktop Optimization Pack (MDOP). App-V gives an organization the ability to make applications available to corporate users without installing the application on the end user's system. App-V allows applications to be managed centrally without the worry of applications conflicting with one another.

App-V allows administrators to deploy applications as services, and App-V allows those applications to be deployed anywhere. App-V allows applications to get transferred from locally installed applications to the cloud.

One real nice advantage of App-V is that when new operating systems and applications get released, there is no need to constantly upgrade your users' systems to run those new applications. Since the applications are virtualized, they can run on older operating systems. When talking about App-V, we need to take a look at some of the components needed. Table 7.3 shows the different components required for App-V.

TABLE 7.3   App-V components

Component	Description
App-V Management Server	Administrators can manage the App-V infrastructure from the Management Server. App-V Management Server allows you to set up virtual applications to the App-V Desktop Client and the Remote Desktop Services Client.
App-V Publishing Server	This server hosts streaming virtual applications and also allows App-V–specific employees to gain access to virtual applications.
App-V Desktop Client	This accesses the virtual applications along with client application publication. Desktop client also manages virtual environments and stores employee-specific application settings.
App-V Remote Desktop Services (RDS) Client	This allows Remote Desktop Session Host servers to work in conjunction with the App-V Desktop Client for shared desktop sessions.
	This is very useful for tablets connecting to corporate applications. If the tablet can't run the application, the tablet user can connect to the Remote Desktop services to access the application.
App-V Sequencer	This tool allows administrators to convert normal applications into virtual applications through the use of a wizard.
Disconnected Operation Mode	The disconnected operation mode allows App-V Desktop Clients to run applications even when the client cannot connect to the App-V Management Server. This allows laptops to continue to access App-V applications even when not connected to the network or the Internet.

Supporting the Windows Store

The Microsoft Windows Store is a one-stop shop for all Microsoft devices. The Windows Store allows users to find and download applications for business and personal use. The Windows Store allows you to download everything from business applications that you can use to create spreadsheets to Xbox games that will allow you to game it out.

You can browse the Windows Store from your PC, tablet, or phone, and you can quickly and easily get free and paid content including games, music, movies, TV shows, and applications. So if your company is looking for free applications to improve business, the Windows Store can help.

One of the advantages to using the Windows Store is that all applications on the store are watched by Microsoft and require a digital certificate to make sure that they are legitimate. If an application is not signed, it will be removed from the Microsoft Store. This also means that you can't build your own apps and place them into the Windows Store without the same security measures. There are methods of loading corporate apps so that only corporate users can gain access to those apps, and that is referred to as sideloading.

Sideloading is the process of loading apps onto your corporate users with the need of a digital signature or the security rules that follow the Microsoft Store.

So what must you do if you want to build your own apps and place them onto the Windows Store? Well, you have to use one of Microsoft's tools that allow you to certify your applications, and those tools include the `MakeCert.exe` and `Pvk2Pfx.exe` tools that are included with the Windows Driver Kit (WDK).

Installing and Managing Software by Using Microsoft Office 365 and Windows Store Apps

One of the best advantages to using the Windows Store is that you can pretty much find and download any application that you need to help your business be more efficient. This can also be one of the biggest issues that an IT department can face. Normally an IT department needs to verify and test all applications before deploying them to the corporate network.

Now your users can find the specific applications that they think will help them do their jobs better and download just those applications. However, IT departments have the ability to turn off the Windows Store through the use of a GPO or local policy, which allows them to maintain more control.

If your IT department does not care about users downloading applications, then the Windows Store is for you. It's very easy to install applications from the Windows Store. You just go to the Windows Store, search for the application that you are looking for, and then click the download button next to that application. Normally the applications will have a small fee associated with them, but many of them are free.

Maintaining and updating applications is also a very easy process. To make sure that your applications get updated whenever there is an update available, just follow these steps:

1. On the Start screen, click the Store icon on the taskbar to open the Windows Store.

2. On the top Windows Store menu, click the picture next to the Search box and then choose Settings.

3. Under App Updates, set the Update Apps Automatically slide bar to On, as shown in Figure 7.8.

FIGURE 7.8 Windows Store Settings
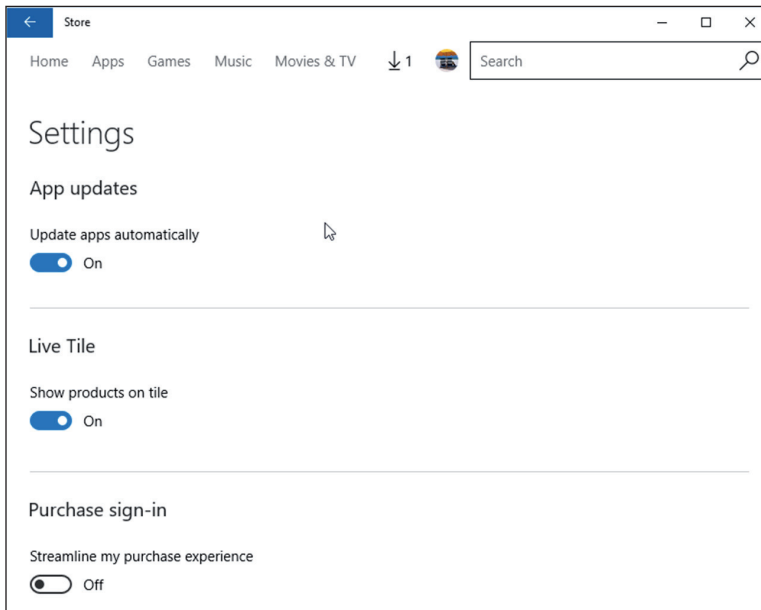
4. When you have finished, close the Windows Store Settings window.

Let's take a look at some of the other things that you can set while on the Settings page for the Windows Store. Users or administrators also have the ability to show products on tiles, require a sign-in for purchases, and manage the devices that are loaded onto the Windows Store.

Now that you know how to get applications from the Windows Store, let's take a look at how to load corporate applications through the process of sideloading.

Sideloading Apps into Online and Offline Images

There will be a time when you or someone in your company may have to build or support a custom-made Line of Business (LOB) application. Companies build and use LOB apps because they have a very special need and can't find a software package to help solve that need.

Sideloading is the process of loading a Windows Store application without needing to publish the software application and download it from the store. Users can install the

software package directly. Windows 10 sideloading has changed since Windows 8 in the following ways:

- Administrators have the ability to unlock a device for sideloading using an enterprise GPO policy.
- Software license keys are not required to install the application.
- Devices do not have to be part of the domain to get an application sideloaded.

Sideloading is not a very difficult process to complete. It is just a few settings along with the use of some PowerShell commands. To enable the systems to accept sideloading, complete the following steps:

1. Open Settings.
2. Click Update & Security ➤ For Developers.
3. Under the Use Developer Features section, choose Sideload Apps, as shown in Figure 7.9.

FIGURE 7.9 Windows sideloading
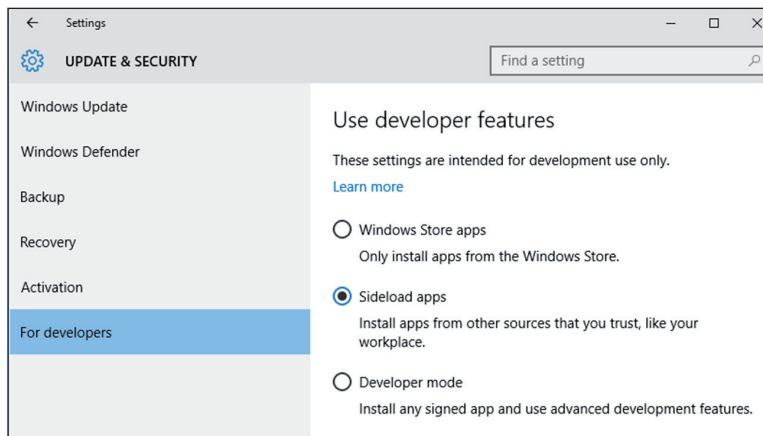
Once the system is enabled to allow applications to be sideloaded, you then need to run some PowerShell commands to make that happen. Navigate to the Windows PowerShell prompt and run the following commands (where "*TestApp*" is the path and name of the package file you created):

```
import-module appx
add-appxpackage "TestApp"
```

Integrating Microsoft Accounts Including Personalization Settings

Normally in the corporate world, we all get issued a corporate username and password so that we can log into the network and access corporate resources. But what if we wanted to access both corporate and personal data from the Internet? That's where integrating your Microsoft online account and your domain account can be beneficial.

Windows 10 gives you the ability to use both a corporate username and personal user account within the same Windows 10 account. Users can link their online accounts with their corporate accounts. So if you have your own personal cloud-based account as well as a corporate account, you can set it up so that you only log in once but have access to both accounts.

Users who decide to link their Microsoft accounts with their corporate accounts have the ability to gain access to applications and games from the Microsoft Windows Store using one account. One of the benefits of tying both accounts together is that once you've completed this setup, the Accounts Wizard will have you establish a PIN at the end. After it's all set, you will log in using the PIN from that point on.

So how do we link the two accounts together? Exercise 7.4 walks you through how to tie both accounts together. After the exercise is complete, your local account will switch to your Microsoft account after you restart your system.

EXERCISE 7.4

Setting the Microsoft Account

1. Click the Start button and then choose Settings. In the Settings window, choose Accounts (shown in Figure 7.10).

FIGURE 7.10   Settings window
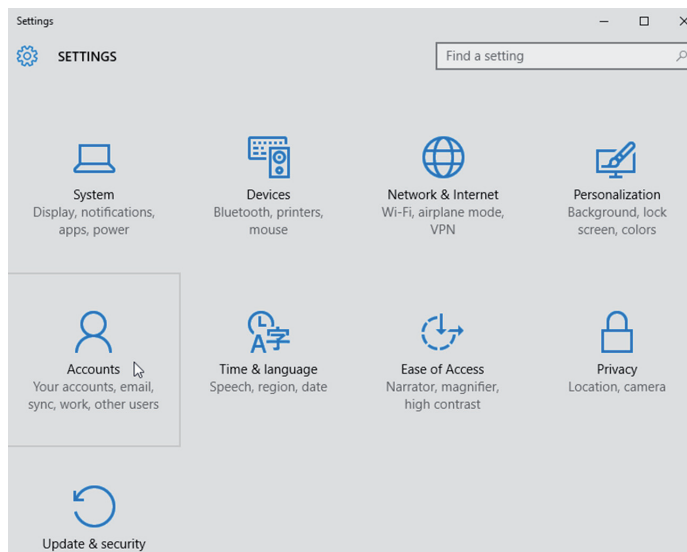
2. In the Accounts window, click the "Sign in with a Microsoft account instead" link (shown in Figure 7.11).

FIGURE 7.11   Accounts window
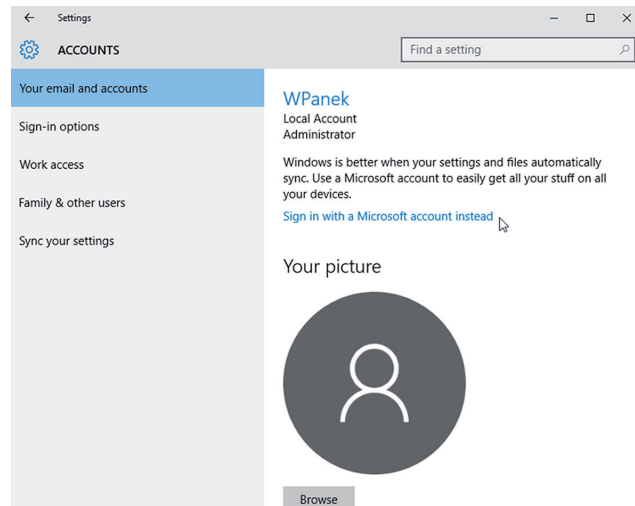
3. A new window will appear that states "Make it your." Type in your Microsoft online username and password. Then click the Sign In button.

4. If a box pops up asking for your Windows network password, enter it and click Next. If you don't have a password, just click Next.

5. The screen will ask you to enter a PIN. Click the Set A PIN button (shown in Figure 7.12) and set your PIN.

FIGURE 7.12   PIN button
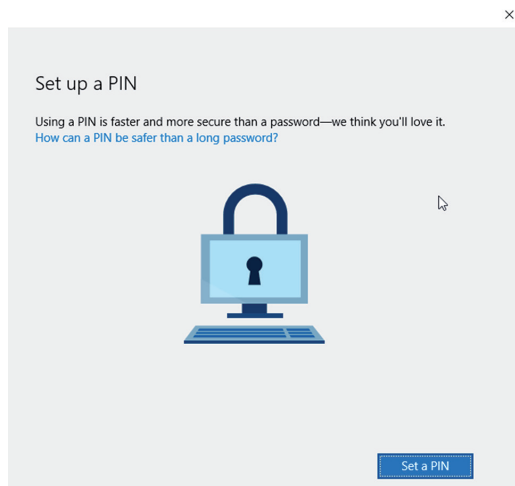
6. After the PIN is completed, you are all set. Close the Accounts window.

Understanding Web Browsers

Windows 10 provides users with two ways to browse the Internet: Edge and IE11. Windows Internet Explorer 11, or IE11, is the latest web browser developed and released by Microsoft Corporation in the popular Internet Explorer series. IE11 is available for Windows 10 and Windows Server 2012 R2 versions.

With the explosion of Internet use—from the inexperienced end users browsing the Internet for personal reasons to those who use it for work-related tasks—enhancing the user interface (UI) while providing better levels of security (which include privacy) has been the focus in the development of both Edge and IE11.

Both browsers are loaded with user features that provide end users with a better and simpler way to get the information they desire from their browsing experience.

The features added to Edge and IE11 are designed to give end users an easy way to browse the Internet for the information they're looking for while providing a secure environment for networks by recognizing potentially bad sites (those attempting to sneak viruses or Trojan horses into the network), phishing sites (those that attempt to steal private information about the user), or invasive sites that users may go to either on purpose or inadvertently.

When comparing the two browsers, Edge and IE11, Edge has taken browsing a step further with the implementation of Cortana. Cortana can assist you while working with Edge.

Browser Controls

When you open either Edge or IE11, one of the first things that will catch your attention is the simplified design. The most common controls, like tools and favorite buttons, are just a click away. You also have the ability to customize how the browser will look and which tools you can use with the browser.

Pinning Sites to the Taskbar

Pinning sites to your taskbar allows you to access the websites by clicking the pinned site at the bottom of the taskbar. Pinning a site is an easy process. Just drag the tab of the website to the taskbar. An icon for the website will stay pinned until you remove it. When you click the pinned icon, the website will open within the Internet browser.

Searchable Address Bar

You have the ability to search the Internet directly from the Address bar. You still have the ability to enter a website's address and go directly to the website. But now you can enter a search term or incomplete address, thus launching a search using your currently selected search engine. You can choose which search engine you want to use by clicking the Address bar and choosing the search engine from the listed icons or adding a new search engine.

Security and Privacy Enhancements

IE11 and Edge have both included many security and privacy enhancements, including some of the following:

- ActiveX Filtering allows you to block ActiveX controls for any sites. You do have the ability to turn them back on for the sites that you trust.

- Domain highlighting allows you to see the real web address of a website you are visiting. This allows you to avoid websites that use misleading web addresses. Domain highlighting is discussed in detail later in this section.

- SmartScreen Filter helps protect users from online phishing attacks, fraud, and spoofed or malicious websites. SmartScreen Filter is discussed in detail later in this section.

- 128-bit Secure Sockets Layer (SSL) connection to use with secure websites.

- InPrivate Browsing allows you to use the Web without saving any data from the websites that are visited while the browser is in this mode.

Working with Web Slices

Web Slices allow your Internet browser (IE, not Edge) to check for updates to web page content you may frequently access. How many times in the course of the day do you check your local weather or stock quotes or even watch an auction item on eBay? Most of the time, you either keep a tab open and refresh it periodically or revisit the website with the content you would like to review.

With Web Slices, you can add the piece of the web page with the content you're looking for to the Favorites bar, and the browser will check it for you when the content changes. With Web Slices, the browser can control how often the browser checks for changes.

Figure 7.13 shows the result of a Bing query for the weather forecast for Portsmouth, New Hampshire, and the Web Slice availability to the Favorites toolbar. Clicking the down arrow associated with the icon will display all of the Web Slices available on the current web page.

FIGURE 7.13   Web Slice
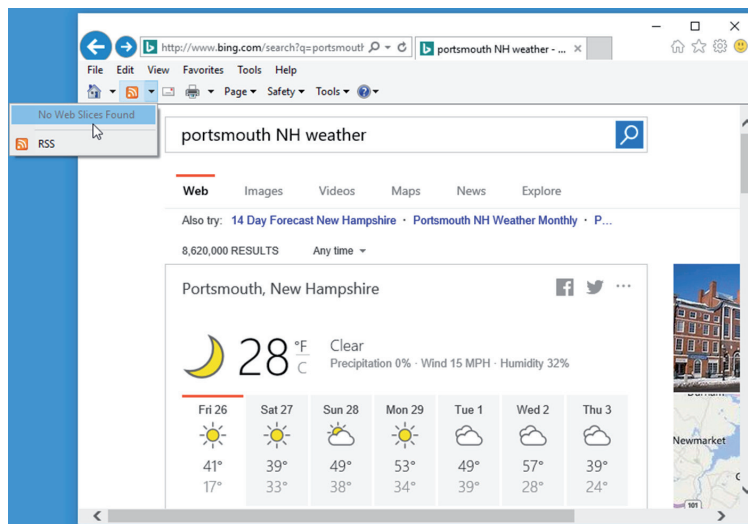
In previous versions of the Internet browsers, Web Slices use to appear within the web page. Now the Web Slices are displayed with the feeds button, as shown in Figure 7.13.

When the user chooses a Web Slice icon, he or she will see a confirmation box for adding the Web Slice to the Favorites bar. Once accepted, the Web Slice is available to be viewed at any time, even after the user browses away from the originating page.

Using the Browser Compatibility View

Windows Internet Explorer 11 is the new release of Microsoft's IE web browser, and some websites may not be updated to use the new features or display their content correctly. Problems may exist displaying misaligned images or text. By using Compatibility View in IE11 (not available in Edge), the browser will display a web page the way it would have been displayed in previous versions, which should correct any display issues. To display a page in Compatibility View, click the Compatibility View option in the tools (shown in Figure 7.14).

FIGURE 7.14   Compatibility View option
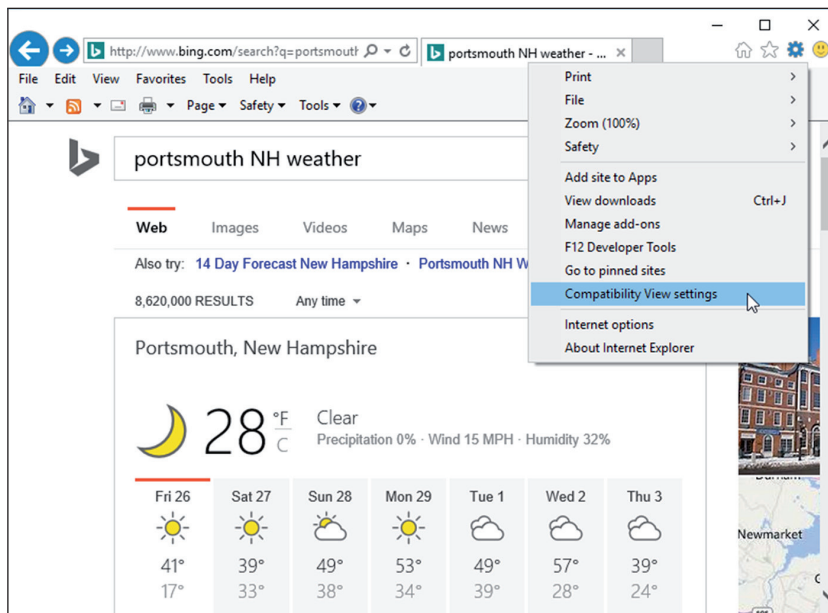
Once you have chosen Compatibility View for a website, you will not need to make the choice again. The browsers will display the site in Compatibility View the next time you browse to it. If the website gets updated in the future or you decide you would prefer to see it in the native standard mode, you can simply click the Compatibility View option again to return to the standard view. The Compatibility View option can also be selected from the Tools menu's Compatibility View menu option.

There is also a Compatibility View Settings option you can use to manage the sites currently set to be viewed in Compatibility View mode by adding or deleting sites by name. Many companies have extensive websites, and it may take time to update them to features. The Compatibility View Settings page has the default setting for all intranet sites to be displayed in Compatibility View. You also have to the choice to display all websites in Compatibility View.

Using Protected Mode for IE11

Protected Mode is a feature of Windows 10 for Windows Internet Explorer 11 that forces IE to run in a protected, isolated memory space, preventing malicious code from directly writing data outside the `Temporary Internet Files` folder unless the program trying to write the information is specifically granted access by the user. Protected Mode is enabled by default and displayed in the lower-right section of Windows Internet Explorer 11.

You can install software through IE11, but you will need to explicitly allow the modification of the file structure of Windows 10 if the software is going to be installed outside the protected directory.

You can change out of Protected Mode from the Security tab of IE11's Internet options (via Tools ➢ Internet Options). You can also open Internet Options by typing **Internet options** into the integrated search box in Windows 10. You also have the option of double-clicking the Protected Mode: On text within Windows Internet Explorer 11 to open just the Security tab of Internet Options.

To toggle Protected Mode, click to select or deselect the Enable Protected Mode check box (this requires restarting Internet Explorer). It is recommended that Protected Mode remain active because it provides a greater level of security and safety for the user and does not prohibit an action (such as installing a program from IE11); it just requires interaction from the user to allow the modification, prompting at least a little thought about what's happening within Windows 10.

Using InPrivate Browsing and InPrivate Filtering

InPrivate Browsing provides some level of privacy to users using Windows Internet Explorer 11 and Edge. The privacy maintained with InPrivate Browsing relates to a current browser where an InPrivate session has been enabled. The InPrivate session prevents the browsing history from being recorded and prevents temporary Internet files from being retained. Cookies, usernames, passwords, and form data will not remain in IE11 following the closing of the InPrivate session, nor will there be any footprints or data pertaining to the InPrivate Browsing session.

InPrivate Browsing keeps information from being saved to the local machine while the session is active, but don't get lulled into a false sense of security; malware, phishing, and other methods that send data out of the local machine are still valid and can provide personal information to a cybercriminal. In addition, employees visiting forbidden sites from work, for instance, could still be detected via forensics.

InPrivate Browsing is a good method of protecting user data if you are not surfing from your own machine or are surfing from a public location (always a bad place to leave personal information). InPrivate Browsing can also be used if you don't want anyone to be able to see data from your Internet browsing session.

There are several ways to launch an IE11 InPrivate Browsing session. One way is to open a new tab and select the Open An InPrivate Browsing Window option from the Browse With InPrivate section. This will open a new tab, and the tab will be an InPrivate session. You can also choose to open Windows Internet Explorer 11 and start an InPrivate session directly by choosing the Safety menu and selecting the InPrivate Browsing menu choice. Alternatively, you can open a new IE11 browser and press Ctrl+Shift+P.

InPrivate Filtering (IE 11 only) takes a slightly different approach in providing security and safety to the user who is surfing using Windows Internet Explorer 11. Many of today's websites gather content from different sources as they present a web page to you. Some of these sources are websites outside the main location, and they provide third-party companies with tracking information about where you surf and what you look at.

This information can then be used to provide statistics as well as send advertisements back to you. InPrivate Filtering provides an added layer of control for the user to decide what information third-party websites will have access to while the user is browsing, limiting the ability of third-party websites to track their browsing usage.

InPrivate Filtering is not enabled by default and must be enabled per browsing session. It is enabled from the Safety menu in IE11. You can alternatively use Ctrl+Shift+F to enable InPrivate Filtering.

The InPrivate Filtering dialog box is an alternate location for enabling InPrivate Filtering or disabling it. You open InPrivate Filtering from the Safety menu of Windows Internet Explorer 11.

Once you choose InPrivate Filtering, you will be given the option to have IE11 automatically block some third-party content or let the user select which third-party providers will receive the user's browsing information. You can always go back and change the options later or turn off InPrivate Filtering if you desire.

After InPrivate Filtering is enabled, you can see which pages have been blocked as third-party queries from the InPrivate Filtering Settings dialog box.

Another advantage of IE11 is that you can configure the web content filter. IE11 also allows you to set up and configure the Allow and Block lists. The Allow and Block lists are lists that you can subscribe to that will automatically filter out certain websites.

Configuring Windows Internet Explorer 11 Options

In addition to security and usability options that you can configure in IE11, you can configure other options for managing the browser. Many of the configurations we have discussed in this chapter (i.e., the Safety or Tools menu options) and have used to quickly change individual parameters are also available for modification within the Internet Options tabbed dialog box. The general parameters, security parameters, privacy configurations, content controls, connection settings, program options, and advanced settings available within Internet Options are discussed in the following sections.

General Parameters

You can open the Internet Properties tabbed dialog box by selecting the Tools menu and choosing the Internet Properties menu item or by simply typing **Internet options** into the integrated search box of Windows 10. The General tab (shown in Figure 7.15) allows you to change the default home page that displays when Windows Internet Explorer 11 is launched. One interesting feature here is that you can have more than one default home page. By entering more than one page in the Home Page text box, each time IE11 is launched, all pages will open in their own tab.

FIGURE 7.15   General tab of IE11's Internet Properties
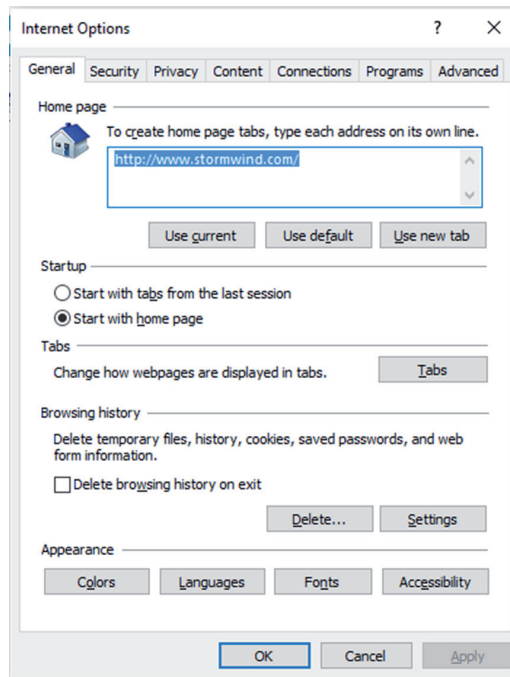
The General tab also allows you to control your Browsing History, Search, Tabs, and Appearance (including accessibility options) settings for the IE11 interface.

Security Parameters

The Security tab of IE11's Internet Properties dialog box (shown in Figure 7.16) not only gives you access to control Protected Mode as discussed earlier in this section but also gives you the ability to set security settings on the specific zones you may browse to as understood by Windows Internet Explorer 11. The zones are the Internet, Local Intranet, Trusted Sites, and Restricted Sites. You can set the behavior of IE11 individually for each zone and even individual sites within each zone. For example, if you add a website to the Local

Intranet settings, you will not be asked to authenticate your credentials when connecting to the website.

FIGURE 7.16   Security tab of IE11's Internet Properties
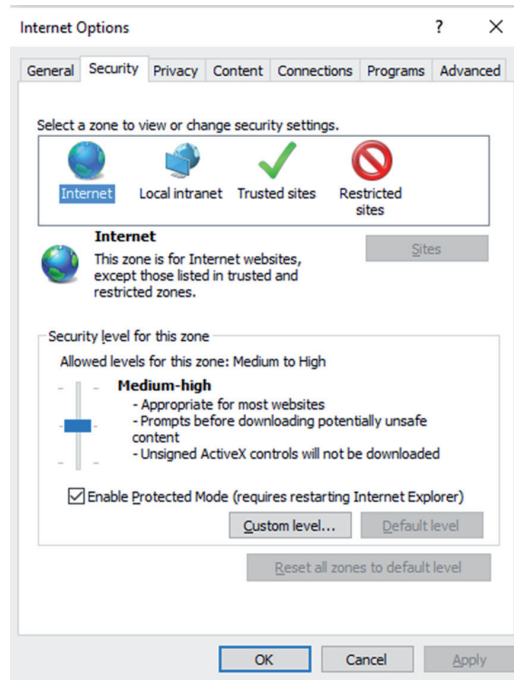
Privacy Configurations

The Privacy tab of IE11's Internet Properties (shown in Figure 7.17) allows the management of privacy settings for the Internet Zone; this is the cookie management for specific sites. You can also control the settings for Pop-up Blocker and your InPrivate Filtering and InPrivate Browsing here.

The Pop-up Blocker allows you to prevent unwanted Internet pop-ups from appearing while you are online. We have all been on websites where pop-up windows start appearing. With the IE11 Pop-up Blocker, you can prevent this from happening. To access the Pop-up Blocker Settings dialog box, click Start ➢ Internet Explorer ➢ Tools ➢ Pop-up Blocker ➢ Pop-up Blocker Settings.

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 IE11 from saving cookies for websites that do not contain a compact privacy policy and cookies that have the potential of saving information that can be used to contact you without your explicit consent. Compact policies are used to indicate the privacy practices of a web service that uses cookies.

FIGURE 7.17   Privacy tab of IE11's Internet Properties
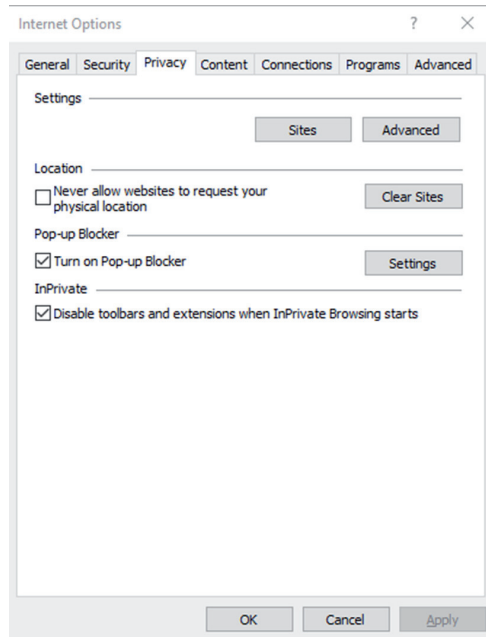
If you want to block any website from accessing cookies stored on the local computer, you should set the privacy setting to Block All Cookies. The Block All Cookies setting prevents cookies from being saved on the computer and prevents any existing cookies from being read by websites.

Content Control

Figure 7.18 shows the Content tab of Windows Internet Explorer 11's Internet Properties. There are Parental Controls to manage which sites are available through web filtering and to monitor website access through an Activity Monitor. There has to be a privileged account with a password set to enforce Parental Controls. InPrivate Browsing is not allowed when Parental Controls are in place.

Content Advisor settings allow a display of rated sites as users browse to different locations. (Sites can be rated based on factors such as fear, tobacco, alcohol, nudity, drugs, gambling, and so on.)

Certificate management for secure browsing is managed through the Content tab as well. You have the ability to manage AutoComplete functionality as well as RSS feeds and Web Slice data from within the Content tab.

FIGURE 7.18   Content tab of the Internet Properties dialog box
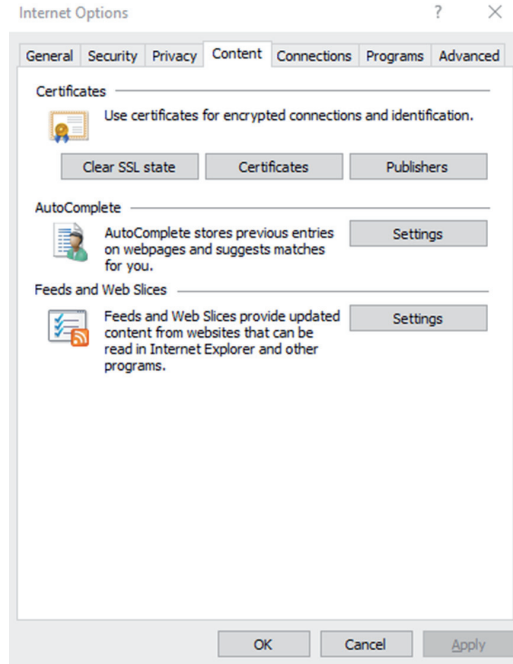
The AutoComplete functionality allows IE11 to automatically fill in fields as you complete forms in IE11. It uses previously entered data to complete the fields on the form.

The Feeds And Web Slices section allows you to fill in what subscription feeds you belong to on the Internet and how often those feeds and slices will be updated along with other configuration options (i.e., playing a sound when the feed or slice is updated).

Connection Settings

The Connections tab of Windows Internet Explorer 11's Internet Properties dialog box allows you to manage the way IE11 gains access to the network. You can initiate the Connect to The Internet Wizard from this tab as well as set up a virtual private network (VPN). If you are using dial-up networking, this connection is also configured from the Connections tab. Local area network (LAN) general settings, which includes specifying a proxy server if you need to use one (this is typical across many corporate sites, to provide a better level of anonymity for Internet surfing), are configured here as well.

Program Options

The Programs tab of the IE11 Internet Properties dialog box allows you to establish a default web browser. You can manage add-ons specific to IE11 in the Programs tab as well.

Additionally, you can set up an application to allow for HTML editing and set up default programs to be used for Internet services such as email.

Advanced Options

The Advanced tab allows you to configure accessibility settings, browsing settings, international browsing settings, encoding settings, multimedia parameters, printing parameters, and general security settings. You can control whether links are underlined, whether pictures should be displayed, which versions of the secure communication protocols or SSL are used, background colors, and many other parameters.

In addition to being able to change the advanced settings, you have the option to restore advanced settings to their original configurations or to even reset Internet Explorer settings, which resets all IE11 settings (not just the advanced settings) to the default configuration.

Summary

Managing Windows software is a very important component that must be properly configured in Windows 10 to guarantee the best possible performance. In the event that the Windows Software packages can't be run on the Windows 10 operating system, there are other options for you to run software with Windows 10.

You can use Hyper-V to create other operating systems on the Windows 10 system. Administrators can also use application virtualization (App-V) to run applications in the cloud. Administrators can also use the cloud to deploy applications by using RemoteApp.

We also talked about how to make sure that applications are going to continue to work properly by testing them through the Application Compatibility Toolkit (ACT).

Another application that is very important to most of us is Internet Explorer. Edge and Internet Explorer 11 are both included with Windows 10, and they have many new features and security enhancements so that the user can get the most out of their browsing experience.

Video Resources

There is a video available for the following exercise:

   7.4

You can access the video at www.wiley.com/go/sybextestprep on the Other Study Tools tab.

Exam Essentials

Understand and know how to install Hyper-V.   Understand what Hyper-V does and know all of the different components of a Hyper-V virtual machine. Understand how to configure virtual machines and the components that make virtual machines operate.

Know how older applications can work in Windows 10.   Understand how to allow older applications to work with Windows 10. You can run applications in Hyper-V or Compatibility Mode or use shims that are created by Microsoft.

Understand how to install applications from the cloud.   You can use Azure RemoteApp to help control and manage how applications get deployed. RemoteApp allows you to download applications to many different Windows device types.

Understand Application Virtualization   Know how to use application virtualization (App-V) and know how to run applications from the cloud without the need to deploy the applications to users' hardware.

Be able to configure privacy settings in IE11 and Edge.   Know how to enable and disable cookies. Know when it is useful to use cookies and when cookies should be blocked. Cookies are files that are placed on your system. Not having files placed on your system increases security. Know how to set an InPrivate session to verify that nothing is saved during an Internet session.

Review Questions

1. You are the network administrator for your organization. Your organization has started using App-V. You notice that laptop users are still able to access App-V applications even when they are not connected to the network. You want to stop this from happening. What do you do?

    A. Disable the Disconnected Operation Mode.

    B. Enable Terminal Services.

    C. Enable Remote Desktop Services.

    D. Discontinue laptops from using App-V.

2. You are the network administrator for your organization. You are asked by your manager to modify the associations of a few file extensions that are associated with Internet Explorer. How can you accomplish this task?

    A. In Control Panel, open Default Programs and then click Set Associations. Set the proper file extensions.

    B. In Internet Explorer, set extensions on the Extension tab.

    C. In Control Panel, open System and then click Set Associations. Set the proper file extensions.

    D. In Internet Explorer, set extensions on the Advanced tab.

3. You are the network administrator for a large organization. You are in charge of implementing company policies. One company policy states that you have to prevent Internet Explorer from saving any data during a user's browsing session. How do you accomplish this?

    A. Set the Internet Security settings to Disabled.

    B. Run the browsers in InPrivate sessions.

    C. Disable InPrivate sessions.

    D. Private sessions should be enabled.

4. You are the network administrator for a large organization. A user calls you and says that when they try to connect to the internal website, they are prompted for authentication. The user has the rights to access the internal site due to the fact that all users and computers are part of a domain and the internal website uses Integrated Windows Authentication. How do you make sure that the user is automatically authenticated when they connect?

    A. Change the user's local permissions to Administrator.

    B. The Local sites URL should be added to the Local Intranet zone.

    C. The Local sites security credentials should be added to the trusted sites zone.

    D. The Internet security level should be lowered to lowest.

5. You are the network administrator for your organization. Your organization has deployed Azure RemoteApp collections by configuring a custom template image. This image is going to contain Microsoft Office 365 ProPlus. Your organization needs to guarantee that multiple employees can run Office 365 ProPlus from the image all at the same time. What do you need to include in your configuration file?

    A. `<Property Name="SHUTDOWNAPP" Value = "True"/>`

    B. `<Property Name="SharedComputerLicensing" Value = "1"/>`

    C. `<Property Name="ACTIVATEAPP" Value = "1"/>`

    D. `<Property Name="OFFICE365ProPlus" Value = "1"/>`

6. Your company has decided to start using AppLocker GPOs to control application access. Jeff, Stormwind's IT Manager, would like to test the AppLocker policy before implementing it. How can Jeff test the AppLocker policy?

    A. In the Group Policy Manager, run the Group Policy Results Wizard.

    B. In the Group Policy Manager, run the Group Policy Modeling Wizard.

    C. In the Group Policy Manager, enforce the new AppLocker policy in Audit-Only mode.

    D. In the Group Policy Manager, run the Group Policy Test Wizard.

7. You are the administrator of an organization who has decided to use Microsoft Azure Active Directory cloud-based services. You have set up a corporate subscription for Microsoft Office 365. Each employee gets a mailbox stored in Office 365 and also an email for the corporate network. After buying out another company, you need to add a third email address to each user. How can you do this?

    A. In Active Directory Sites And Services, edit the email attribute for each employee.

    B. In Active Directory Domains And Trusts, edit the email attribute for each employee.

    C. Use the `Set-Mailbox` cmdlet from the Azure Active Directory Module for PowerShell.

    D. Use the `Set-Mailbox` cmdlet from the Active Directory Module for PowerShell.

8. You are the network administrator for a large organization. You have installed Hyper-V on a server called ServerA, and you have set up four new VM servers. You want to run PowerShell commands for the VM servers from ServerA. How do you do this?

    A. Use the `Invoke-Command` cmdlet and specify the `VMName` parameter.

    B. Use the WinRM command `-PowerShell`.

    C. Use the PSCommands–enabled command.

    D. Just run the PowerShell commands with the `-Name` parameter.

9. You are the network administrator for a large organization. You have deployed a software package to all of the Windows computers in your domain. You want to set up a GPO so that some employees have no access to the application. How do you accomplish this?

    A. Set up a restriction server and place all of your restricted employees onto that server.

    B. Configure BitLocker.

    C. Configure AppLocker.

    D. Configure each Windows 10 system to use user policies.

10. You are the administrator of a large organization. Your company has developed an application for your employees. You need to deploy the internally developed application to all employees while minimizing the costs. What's the best way to do that?

A. Install the application one system at a time.

B. Enable application sideloading.

C. Purchase System Center and deploy the application.

D. Run the `Add-Application` PowerShell cmdlet.

Chapter

8

Managing Identity and Authorization

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Support authentication and authorization.**

- This objective may include but is not limited to: Identifying and resolving issues related to the following: Multi-factor authentication including certificates, Microsoft Passport, virtual smart cards, picture passwords, and biometrics; workgroup vs. domain, Homegroup, computer and user authentication including secure channel, account policies, credential caching, and Credential Manager; local account vs. Microsoft account; Workplace Join; Configuring Windows Hello.

This may be one of the most important chapters in this study guide. Setting up users, groups, and security involves some of the most critical tasks that any IT manager needs to perform.

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 10, users can log on to a computer locally, or if the machine is a member of an Active Directory domain, the user can authenticate against a local copy of Active Directory or a cloud-based copy of Active Directory.

Groups are used to ease network administration by grouping users who have similar permission requirements. 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 10 includes built-in local groups, such as Administrators and Backup Operators.

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.

Windows 10 also offers a wide variety of security options. If the Windows 10 computer is a part of a domain, you can apply security through Group Policy Objects using the Group Policy Management Console. If the Windows 10 computer is not a part of a domain, then you can use Local Group Policy Objects to manage local security.

Overview of Windows 10 User Accounts

When you install Windows 10, several user accounts are created automatically. Additionally, you can create new user accounts. As you already know, user accounts allow a user to log on to machines and access resources.

You can create local user accounts, which reside locally on the Windows 10 machine. Such accounts cannot be utilized to gain access to any resources hosted on the network. If you have installed Active Directory either in the cloud (Azure Active Directory) or on a network that has a Windows Server 2012/2012 R2, Windows Server 2008/2008 R2, Windows Server 2003, or Windows Server 2000 domain controller, your network can have domain user accounts as well.

In the following sections, you will learn about the different account types: the default user accounts that are created by Windows 10 and the difference between local and domain user accounts.

Account Types

Windows 10 supports two basic types of user accounts: administrator and standard user (see Figure 8.1). Each of these accounts is used for specific reasons.

FIGURE 8.1   Choosing an account type
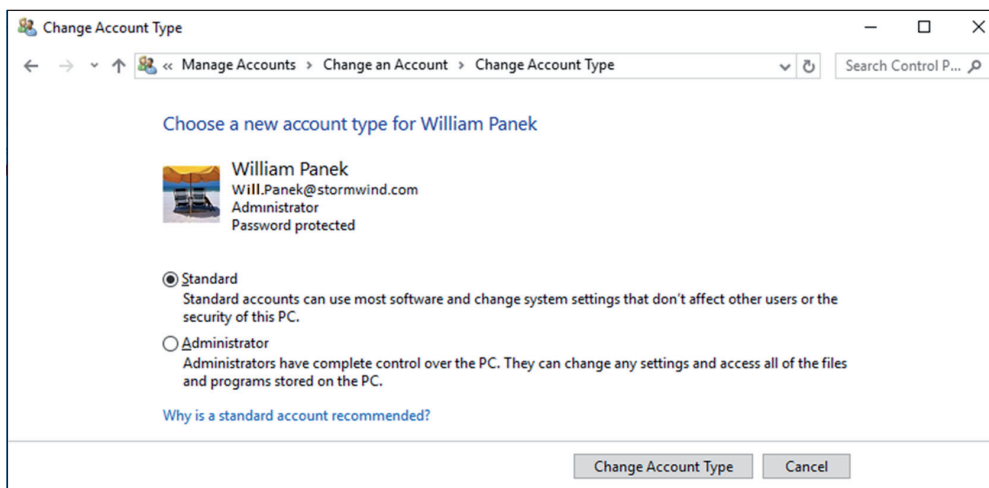
Administrator   The administrator account type provides unrestricted access for performing administrative tasks. As a result, administrator accounts should be used only for performing administrative tasks and should not be used for normal computing tasks.

Only administrator accounts can change the Registry. This is important to know because when most software is installed onto a Windows 10 machine, the Registry gets changed. This is why you need administrator rights to install most software.

Standard User   The standard user account type should be assigned to every user of the computer. Standard user accounts can perform most day-to-day tasks, such as running Microsoft Word, accessing email, 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. Standard user accounts are unable to make system-wide changes, which also helps to increase security.

When you install Windows 10, by default, there are premade accounts called built-in accounts. Let's take a look at them.

Built-In Accounts

When installed into a workgroup environment, Windows 10 has five built-in accounts, which are created automatically at the time you install the operating system (see Figure 8.2). Figure 8.2 also shows the accounts that I created while writing this book.

FIGURE 8.2 The five built-in accounts
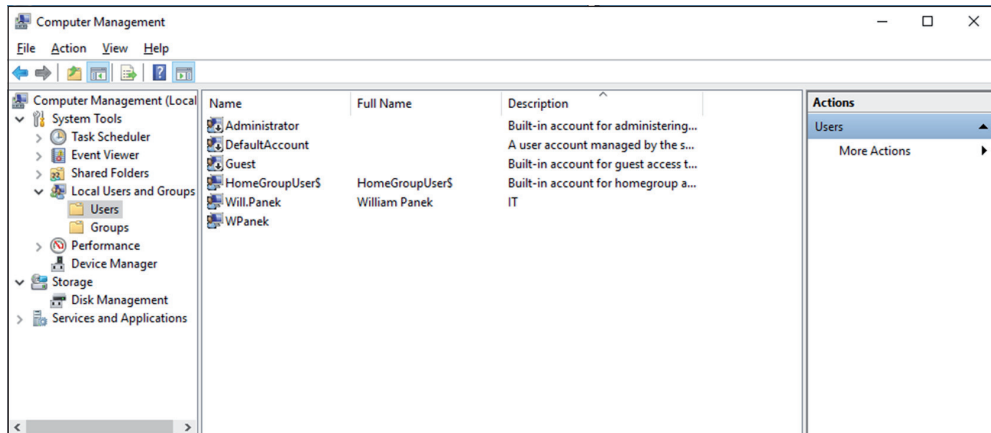
Administrator The Administrator account is a special account that has full control over the computer. The Administrator account can perform all tasks, such as creating users and groups, managing the filesystem, installing applications, and setting up printing. Note that the Administrator account is disabled by default.

DefaultAccount This is a user account created by the system and used by the system. This account is a member of the HomeUsers group and the System Managed Accounts group.

Guest The Guest account allows users to access the computer even if a person does 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.

**HomeGroupUser$** The HomeGroupUser$ account is created by default to allow this machine to connect to other machines within the same HomeGroup network. This account is created by default as soon as you set up a HomeGroup.

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 10, this user account is disabled by default. You can increase the computer's security by leaving this account disabled and assigning other users to the Administrators group. This way, a malicious user will be unable to log on to the computer using the Administrator user account.

All five of these users are considered local users, and their permissions are contained to the Windows 10 machine. If the user's account needs to access resources on machines other than their own, you can have a user log in to the Windows 10 computer as a remote user (a user who is not in front of the machine they're logging on to), and this would be considered a domain user's account. Let's take a look at the difference between these account types.

Local and Domain User Accounts

Windows 10 supports two kinds of users: local users and domain users. Local users get set up on each Windows 10 client system. The Windows 10 system can be part of a workgroup or it can be a stand-alone system. A computer that is running Windows 10 has the ability to store its own user accounts database. The user accounts stored at the local computer are known as *local user accounts*.

Workgroups are networks that have user databases on each individual Windows 10 machine. However, you can share resources on the workgroup network.

Domains

Domains are networks where there is a centralized security database (Active Directory), and you can control all of your users and groups from one central location.

Active Directory is a directory service that stores information in a central database, which allows users to have a single user account for the network. The user accounts stored in Active Directory's central database are called *domain user accounts*. Active Directory is available in two different models. There is a cloud-based Active Directory called Azure Active Directory and a server-based version that runs on Windows Server 2012/2012 R2, Windows Server 2008/2008 R2, Windows Server 2003, and Windows 2000 Server platforms.

Workgroups

You can log on locally to a Windows 10 computer using a locally stored user account, or you can log on to a domain using an Active Directory account. When you install Windows 10 on a computer, you specify that the computer will be a part of a workgroup, which implies a local logon, or that it will be a part of a domain, which implies a domain logon.

On all Windows versions except domain controllers, you can create local users through the Local Users and Groups utility, as described in the section "Working with User Accounts" later in this chapter. On Windows Server domain controllers (Windows Server 2000 and above), you manage users with the Microsoft Active Directory Users and Computers MMC.

Active Directory is covered in detail in *MCSA Windows Server 2012 R2 Complete Study Guide: Exams 70-410, 70-411, 70-412, and 70-417*, by William Panek (Sybex, 2016).

Workplace Join

There may be times when you need someone to gain access to a domain resource but that person doesn't have a domain account. That's where Workplace Join can help. Workplace Join is a Windows tool that you can download and use on your domain.

Workplace Join allows an end user to use a corporate email address and password to connect a Windows system (Windows phone, tablet, or operating system) to a domain. The email address and password are then sent to an Active Directory server to be verified. The server can be set to then send a message to the device to confirm that the device should be given access to the domain. After the verification is done, Workplace Join creates a new device object in Active Directory and installs a certificate onto the Windows device.

Logging Off

No matter what type of network you have, you will eventually need to log off the Windows 10 system. When users are ready to stop working, they should either log off or shut down the system. A user can do either of these by right-clicking the Windows Start button and choosing Shut Down or Sign Out.

Working with User Accounts

To set up and manage your local user accounts, you use the Local Users and Groups utility or the User Accounts option in Control Panel. With either option, you can create, disable, delete, and rename user accounts as well as change user passwords.

Windows 10 includes User Account Control (UAC), which 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.

Using the Local Users and Groups Utility

There are two common methods for accessing the Local Users and Groups utility:

- Load Local Users and Groups as a Microsoft Management Console (MMC) snap-in.
- Access the Local Users and Groups utility through the Computer Management utility.

If your computer doesn't have a custom MMC configured, the quickest way to access the Local Users and Groups utility is through the Computer Management utility.

In Exercise 8.1, you will add the Local Users and Groups snap-in MMC to the desktop. This exercise needs to be completed in order to complete other exercises in this chapter.

EXERCISE 8.1

Adding the Local Users and Groups Snap-in

1. In the Search box, type **MMC** and press Enter.

2. If a warning box appears, click Yes.

3. Select File ➤ Add/Remove Snap-in.

4. Scroll down the list and highlight Local Users And Groups, and then click the Add button (shown in Figure 8.3).

FIGURE 8.3   MMC snap-ins
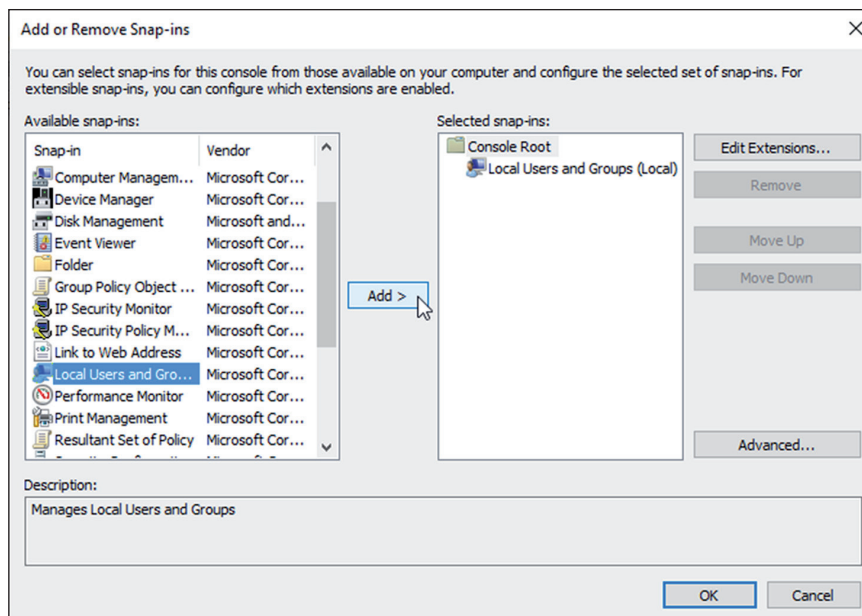
5. In the Choose Target Machine dialog box, click the Finish button to accept the default selection of Local Computer.

6. Click OK in the Add Or Remove Snap-ins dialog box.

7. In the MMC window, right-click the `Local Users And Groups` folder and choose New Window From Here. You will see that Local Users and Groups is now the main window.

8. Click File ➤ Save As. Name the console **Local Users and Groups** and choose Desktop under the Save In pull-down box. Click the Save button. This is creating the shortcut shown in Figure 8.4 for you to use in exercises throughout this chapter.

FIGURE 8.4 Local Users and Groups MMC
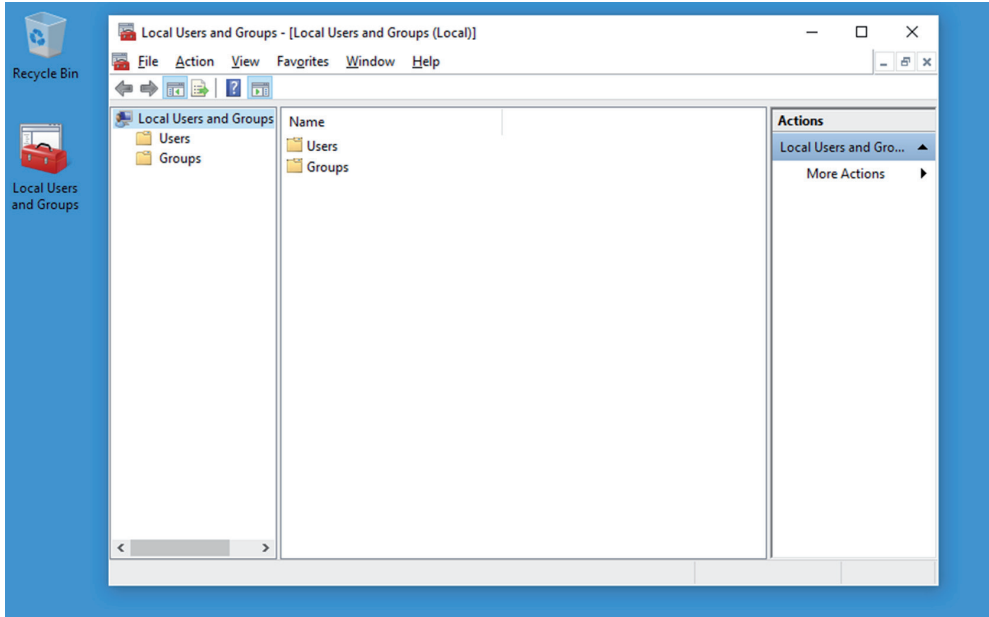
9. Close the MMC snap-in. You should now see the Local Users and Groups snap-in on the Desktop. You can also open the Local Users and Groups MMC from the Computer Management utility, which you'll do in Exercise 8.2. Complete the following exercise for opening the Local Users and Groups utility from the Computer Management utility.

EXERCISE 8.2

Accessing Local Users and Groups via the Computer Management Utility

1. Right-click the Start button and then choose Computer Management.

2. In the Computer Management window, expand the `System Tools` folder and then the `Local Users and Groups` folder.

Using the User Accounts Option in Control Panel

Now let's look at an alternative way to configure local users and groups through the *User Accounts Control (UAC)* Control Panel option, which provides the ability to manage user accounts in addition to configuring parental controls. To access the User Accounts Control

Panel option, right-click Start ➤ Control Panel ➤ User Accounts. Table 8.1 briefly describes the configurable options in the User Accounts option in Control Panel.

TABLE 8.1 Configurable user-account options in Control Panel

Option	Explanation
Change Your Password	Allows you to change a user's password.
Change Your Account Name	Allows you to rename the account.
Change Your Account Type	Allows you to change your account type between the standard user and administrator account type.
Manage Another Account	Allows you to configure other accounts on the Windows 10 machine.
Change User Account Control Settings	Allows you to set the level of notification displayed through pop-up messages when changes are made to your computer. These notifications can prevent potentially hazardous programs from being loaded onto the operating system.
Manage Your Credentials	Allows you to set up credentials so you can easily connect to websites that require usernames and passwords or computers that require certificates.
Manage Your File Encryption Certificates	Allows you to manage your file-encryption certificates.
Configure Advanced User Profile Properties	Takes you directly to the User's Profile dialog box in Control Panel ➤ System ➤ Advanced ➤ System Settings.
Change My Environment Variables	Allows you to access the Environment Variables dialog box directly.

Creating New Users

To create users on a Windows 10 computer, you must be logged on as a user with permission to create a new user, which means your account must be a member of the Administrators group.

When you create a new user, there are many options that you have to configure. Table 8.2 describes all the options available in the New User dialog box. (You access this dialog box through the MMC, which is detailed in Exercise 8.3 later in this chapter.)

TABLE 8.2   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., WPanek). This is the only required field. Usernames are not case-sensitive.
Full Name	Allows you to provide more-detailed name information. This typically consists of the user's first and last names (e.g., Will Panek). 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.
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 he or she logs 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. This 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.

In the following sections, you will learn about username rules and conventions and security identifiers.

Username Rules and Conventions

The only real requirement for creating a new user is that you provide a valid username. To be valid, the name must follow the Windows 10 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 10 rules for usernames:

- A username must be from 1 to 20 characters.

- The username must be unique among all the other user and group names stored on the computer.

- The username cannot contain any of the following characters:

    / \ [ ] : ; | = , + ? < > " @

- A username cannot consist exclusively of periods or spaces.

Keeping the Windows 10 rules in mind, you should choose a naming convention (a consistent naming format) for your company. For example, your naming convention might be to use the last name and first initial, so for a user named William Panek, the username would be WillP or WilliamP. Another naming convention might use the first initial and last name, for the username WPanek. This is the naming convention followed by many midsize and larger organizations. You could base usernames on the naming convention your company has defined for email names so that the logon name and the name in the email address match.

You should also provide a mechanism that will accommodate duplicate names. For example, if you have a user named Jane Smith and a user named John Smith, you might use a middle initial for usernames, such as JDSmith and JRSmith. It is also a good practice to come up with a naming convention for groups, printers, and computers.

🌐 Real World Scenario

Naming-Convention Considerations

As an IT manager, I don't recommend using first name, first initial of last name (WilliamP) as a naming convention. In a midsize-to-large company, there is the possibility of having two WilliamPs, but the odds that you will have two WPaneks are rare.

If you choose to use the first name, first initial of last name option, it can be a lot of work to go back and change this format later if the company grows. Choose a naming convention that can grow with the company.

When creating users, it's important to make sure that your usernames and passwords are as strong as possible. The reason that you want strong security is because when a user logs into a system, the user's credentials are placed into the computer's Local Security Authority

Subsystem Service (LSASS) process memory. This is done so that the credentials can be used by the account during a session connection.

Credentials will also get stored on the Windows 10 authoritative databases, such as the SAM database and in the database that is used by Active Directory Domain Services (AD DS). Therefore, it's important to make your usernames and passwords strong so that hackers have the hardest time to hack into a system and steal these cached credentials.

Now let's take a look at how user accounts get security ID numbers associated with them and how those numbers affect your accounts.

Security Identifiers

When you create a new user account, a *security identifier (SID)* is automatically created 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 10 uses the SID as the user object, you can easily rename a user while retaining all the user's properties. All security settings get associated with the SID, not the user account. Every time you create a new user, a unique SID gets associated. This ensures 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. Even if the username is the same as a previously deleted account, the system still sees the account as a new user.

Because every user account gets a unique SID number, it is a good practice to disable rather than delete accounts for users who leave the company or have an extended absence. If you ever need to access the disabled account again, you have the ability to do so.

Secure Channel

Another part of authentication and encrypted communications between a client and a server is a mechanism called *Secure Channel*. Secure Channel, also known as Schannel, is a set of security protocols that help offer secure encrypted communications and authentication between a client and a server.

Schannel is a security package that uses the following four protocols on the Windows platforms:

- Transport Layer Security (TLS 1.1)
- Transport Layer Security (TLS 1.2)
- Secure Sockets Layer (SSL 3.0)
- Secure Sockets Layer (SSL 2.0)

To create a Schannel connection, the clients and servers are both required to obtain Schannel credentials and create a security session. Once the client and server connection is obtained, the security credentials become available. If a connection is lost for any reason, the client and server can automatically renegotiate the connection and finish all communications.

Creating a New Local User Account
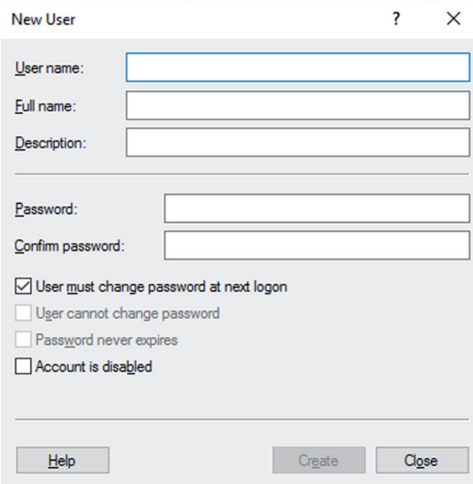
Complete Exercise 8.3 to create a new local user account. Before you complete the following steps, make sure you are logged on as a user with permissions to create new user accounts and have already added the Local Users and Groups snap-in to the MMC (Exercise 8.1). I created bogus usernames; you can change these to whatever names you want to use, but I refer to the ones I created in other exercises.

EXERCISE 8.3

Creating New Users via the MMC

1. Open the Local Users and Groups MMC Desktop shortcut that you created in Exercise 8.1, and expand the Local Users and Groups snap-in. If a dialog box appears, click Yes.

2. Highlight the Users folder and select Action ➢ New User. The New User dialog box appears, as shown in Figure 8.5.

FIGURE 8.5   New User dialog box

3. In the User Name text box, type **APanek**.

4. In the Full Name text box, type **Alexandria Panek**.

5. In the Description text box, type **Operations Manager**.

6. Leave the Password and Confirm Password text boxes empty. Make sure you uncheck the User Must Change Password At Next Logon option, and accept the defaults for the remaining check boxes. Click the Create button to add the user.

7. Use the New User dialog box to create four more users, filling out the fields as follows:

> User Name: **PPanek**; Full Name: **Paige Panek**
>
> User Name: **GWashington**; Full Name: **George Washington**
>
> User Name: **JAdams**; Full Name: **John Adams**
>
> User Name: **ALincoln**; Full Name: **Abe Lincoln**

8. After you've finished creating all of the users, click the Close button to exit the New User dialog box.

> **NOTE** You can also create users through the command-line utility NET USER. For more information about this command, type **NET USER /?** at the 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 reenable it to restore it with all of its associated user properties. An account that is deleted, however, can never be recovered unless you complete a restore from a backup.

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 and would like to reuse the account.

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), enable it, and reset the password. 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 is laying off a group of people, as a security measure you could disable their accounts at the same time the layoff notices are given out. This

prevents those users from inflicting any damage to the company's files after they receive their layoff notice. (Note, however, that this won't affect users who are already logged in.)

In Exercise 8.4, you will disable a user account. Before you complete this exercise, you should have created new users in Exercise 8.3.

EXERCISE 8.4

Disabling User Accounts

1. Open the Local Users and Groups MMC Desktop shortcut that you created in Exercise 8.1 and expand the Local Users and Groups snap-in.

2. Open the Users folder. Double-click user PPanek to open her Properties dialog box.

3. In the General tab, check the Account Is Disabled box. Click OK.

4. Close the Local Users and Groups MMC.

5. Log off and attempt to log on as PPanek. This should fail because the account is now disabled.

6. Log back on using your user account.

> **NOTE** You can also access a user's properties by highlighting the user, right-clicking, and selecting Properties.

When a user has left the company for a long period of time and you know you no longer need the user account, you can delete it. Let's take a look at how to delete user accounts.

Deleting User Accounts

As noted in the preceding section, you should disable a user account if you are not sure whether the account will ever be needed again. But if the account has been disabled and you know that the user account will never need to be accessed again, you should delete the account.

To delete a user, open the Local Users and Groups utility, highlight the user account you wish to delete, click Action to bring up the menu shown in Figure 8.6, and then select Delete. You can also delete an account by clicking the account and pressing the Delete key on the keyboard.

FIGURE 8.6   Deleting a user account
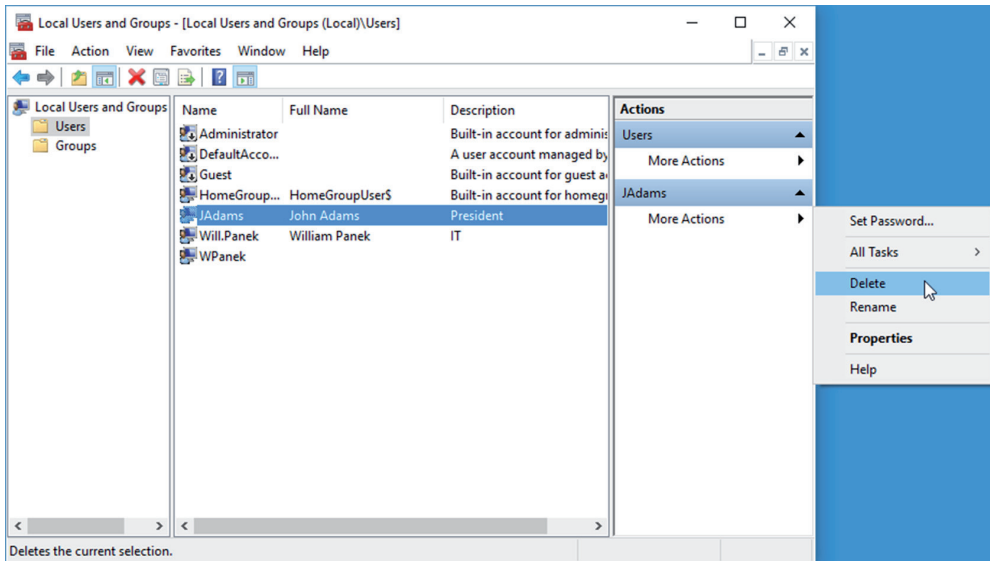
Because deleting an account is a permanent action, you will see the dialog box shown in Figure 8.7, asking you to confirm that you really wish to delete the account. After you click the Yes button here, you will not be able to re-create or reaccess the account (unless you restore your local user accounts database from a backup).

FIGURE 8.7   Confirming account deletion
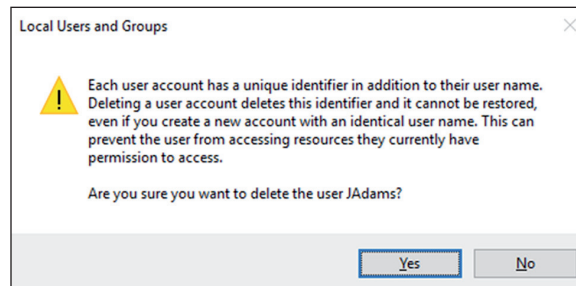
Complete Exercise 8.5 to delete a user account. These steps assume you have completed Exercises 8.2, 8.3, and 8.4.

EXERCISE 8.5

Deleting a User Account

1. Open the Local Users and Groups MMC Desktop shortcut and expand the Local Users and Groups snap-in.

2. Expand the `Users` folder and single-click user JAdams to select his user account.

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.

5. Close the Local Users and Groups MMC.

Now that you have disabled and deleted accounts, let's take a look at how to rename a user's account.

Renaming User Accounts

Once an account has been created, you can rename it at any time. Renaming a user account allows the account to retain all the associated user properties such as group memberships and assigned permissions even though the username is being changed.

You might want to rename a user account because the user's name has changed, for example, the user gets married, or because the name was spelled incorrectly. Also, as explained in the section "Disabling User Accounts," 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.

Complete Exercise 8.6 to rename a user account. These steps assume you have completed Exercises 8.2 through 8.5.

EXERCISE 8.6

Renaming a User Account

1. Open the Local Users and Groups MMC Desktop shortcut and expand the Local Users and Groups snap-in.

2. Open the `Users` folder and highlight user ALincoln.

3. Select Action ➢ Rename.

4. Type the username **RReagan** and press Enter. Notice that the Full Name field retains the original Full Name property of Abe Lincoln in the Local Users and Groups utility.

5. Double-click RReagan to open the properties and change the user's full name to Ronald Reagan.

6. Click the User Must Change Password At Next Logon check box.

7. Click OK.

8. Close the Local Users and Groups MMC.

Renaming a user does not change any hard-coded names, such as the name of 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. (Note that there is a small possibility that you'll have to change the Registry to point to the new name.)

Another very common task that we must deal with is changing the user's password. Let's take a look at how to do that.

Changing a User's Password

What should you do if a user forgets his or her password and can't log on? As the administrator, you can change the user's password, which he or she can then use.

It is very important as IT managers and IT administrators that we teach our users proper security measures that go along with password protection. As you have all probably seen before, the users who tape their password to their monitors or under the keyboards are not following correct security precautions. It's our job as IT professionals to teach our users proper security, and it always amazes me when I do consulting how many IT departments don't teach their users properly.

Complete Exercise 8.7 to change a user's password. This exercise assumes you have completed Exercises 8.2 onward.

Changing a User's Password

1. Open the Local Users and Groups MMC Desktop shortcut and expand the Local Users and Groups snap-in.

2. Open the Users folder and highlight user APanek.

3. Select Action ➢ Set Password. The Set Password dialog box appears.

4. A warning appears, indicating the risks involved in changing the password. Select Proceed.

5. Type the new password and then confirm the password. Click OK.

6. Close the Local Users and Groups MMC.

Using a Microsoft Passport, Pictures, and Biometrics

Now that we have looked at how to set up and manage local and domain accounts, let's look at how you can use other options to help you log into your system or network.

Those of us who have been certified for a long time are quite familiar with using a Microsoft account to log into the Microsoft websites. Now we can use this same account to log into our computer and networks.

Microsoft Passports are Microsoft accounts that you can use to authenticate to a domain, to a cloud-based domain, or to a computer. To do this, you need to link your Microsoft account to your Windows 10 system.

Linking your Windows 10 system is an easy two-step verification process with Microsoft Passport enrollment. When you set up a Microsoft Passport on the device, you can set up the system to use Windows Hello or a PIN.

Windows Hello allows you to sign in to your Windows 10 devices with just a look or a touch. Windows Hello can be set up so that you can use biometrics, face recognition, or even an iris scan. To configure Windows Hello options, click the Start menu and choose Settings. Once you're in the settings, choose Accounts.

You also have the ability to set up Microsoft Passport to use a PIN number. This is a secure number that you input instead of a username and password. You may be thinking to yourself that a PIN doesn't seem as secure as a username and password, but actually that is not true.

PINs can be very complex and include special characters and letters, both uppercase and lowercase. So that means that you can have a PIN of 1234 or a PIN of 1234Wi!!Panek1001. Also, PINs are tied directly to a machine and not to an account, so when you set up a PIN, it's good for that machine only. Because of this, PINs are actually better than a password that can be used anywhere on the network. If someone steals your password, they can access your account from anywhere. This is not the case with a PIN, because anyone trying to use it would also need access to your machine.

Windows 10 also gives you the ability to set up your logon for use with a picture. When you decide to use a picture for authentication, you first choose your picture and then you add three gestures onto the picture. You can draw straight lines, circles, squares, or anything you want. Then when you log on to the system, you just re-create the gestures on the picture and the system logs you in.

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 user 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 contains the information you supplied when you set up the new user account, including the full name and a description, the password options you selected, and whether the account is disabled. 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 (Figure 8.8).

FIGURE 8.8 General tab of the user's Properties dialog box
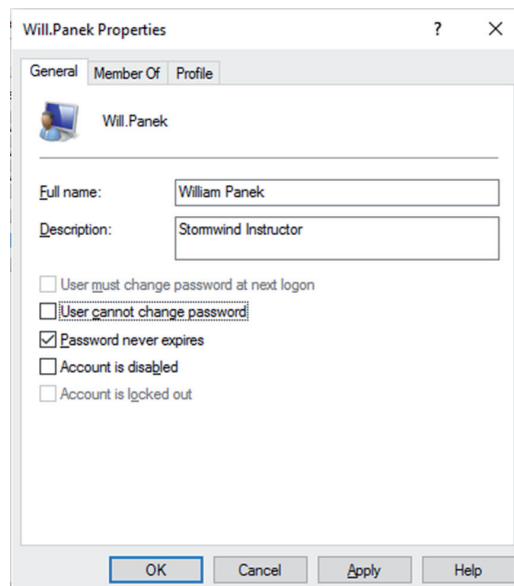
You can use the Member Of tab to manage the user's membership in groups, and the Profile tab lets you set properties to customize the user's environment. The following sections discuss the Member Of and Profile tabs in detail.

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 8.9. From this tab, you can add the user to an existing group or remove the 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 8.9   The Member Of tab of the user's Properties dialog box
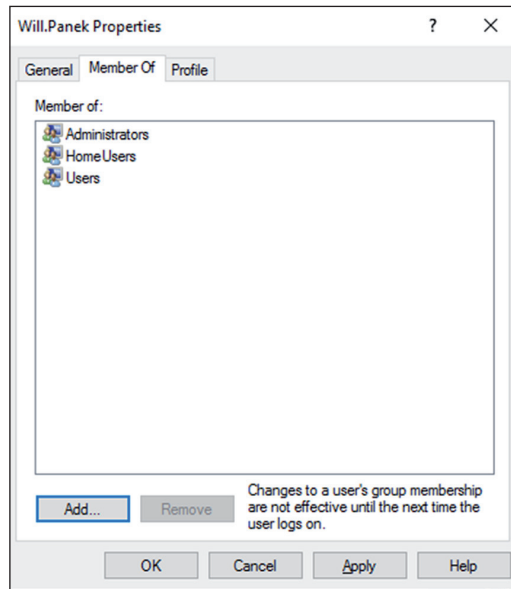
Complete Exercise 8.8 to add a user to an existing group. These steps assume you have completed Exercises 8.2 onward.

EXERCISE 8.8

Adding a User to an Existing Group

1. Open the Local Users and Groups MMC Desktop snap-in that you created previously.

2. Open the Users folder and double-click user APanek. The APanek 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 the Check Names button. After the name is confirmed, click OK.

5. Click OK to close the APanek Properties dialog box.

Now let's take a look at the Profile tab and what options can be configured within that tab.

Setting Up User Profiles, Logon Scripts, and Home Folders

The Profile tab of the user's Properties dialog box, shown in Figure 8.10, 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

FIGURE 8.10 The Profile tab of the user's Properties dialog box
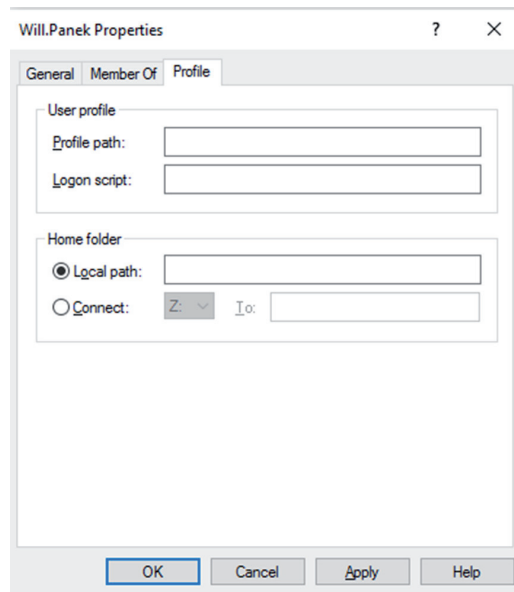
The following sections describe how these properties work and when you might want to use them.

Setting a User's Profile Path

User profiles contain information about the Windows 10 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 10 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 10. 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 (as shown previously in Figure 8.10).

In Exercise 8.9, you'll create two new users and set up local user profiles.

EXERCISE 8.9

Setting Up User Profiles

1. Using the Local Users and Groups utility, create two new users: WPanek and CPanek. Deselect the User Must Change Password At Next Logon option for each user.

2. Select Start ➢ All Programs ➢ Accessories ➢ Windows Explorer. Expand Computer ➢ Local Disk (C:) ➢ Users. Notice that the `Users` folder does not contain user profile folders for the new users.

3. Log off and log on as WPanek.

4. Right-click an open area on the Desktop and select Personalize. In the Personalization dialog box, select a color scheme and 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** to open the Calculator program. Accept CALC as the name for the shortcut and click Finish.

6. Log off as WPanek and log on as CPanek. Notice that user PPanek sees the Desktop configuration stored in the default user profile.

7. Log off as CPanek and log on as WPanek. Notice that WPanek sees the Desktop configuration you set up in steps 3, 4, and 5.

8. Log off as WPanek and log on as your user account. Open Windows Explorer. Expand Computer ➢ Local Disk (C:) ➢ Users. Notice that this folder now contains user profile folders for WPanek and CPanek.

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 10 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. To enable 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 because they can't be stored on a local Windows 10 computer.

In the next sections, you will learn about how roaming profiles and mandatory profiles can be used. To have a roaming profile or a mandatory profile, your computer must be a part of a network with server access.

Using Roaming Profiles

A *roaming profile* is stored on a network server and allows a user 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.

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 can create mandatory profiles for a single user or a group of users. 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, which they will not be able to change.

The mandatory profile is stored in a file named `NTUSER.MAN`. To create a mandatory profile, you just change the user's profile extension to `.man`, and the profile will become mandatory. 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.

There are two folders where the profiles are stored. They are *Username* and *Username*.v2 (*Username* will be replaced with the user's name). The difference is that if you are using Windows XP, the profile gets placed in the *Username* folder. If the users are using Windows Vista, Windows 7/8/8.1, Windows 10, or Windows Server 2008, the user profile gets placed in the *Username*.v2 folder.

> **NOTE** You can use only roaming profiles as mandatory profiles. Mandatory profiles do not work for local user profiles.

Now let's look at a second type of mandatory profile called super-mandatory profile.

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 that for creating mandatory profiles, except that instead of renaming the user folder *Username*.v2 as you would for a mandatory profile, you name the folder *Username.man*. User profiles become *super-mandatory* when the folder name of the profile path ends in .man, for example, \\server\ share\APanek.man\. Only system administrators can make changes to mandatory user profiles.

🌐 Real World Scenario

Copying User Profiles

Within your company, you have a user, Paige, 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 Paige 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 Paige's administrative account to her regular user account) by choosing Control Panel ➢ System ➢ Advanced System Settings ➢ User Profiles Settings. 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

Another configurable element within the Profile tab of the user's properties is logon scripts—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. Logon scripts are either created by the admin or just grabbed off the Internet. Creating these scripts is beyond the scope of this book.

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 10 operating systems for users 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.

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. The main reason you give your users a home folder on the server is because the servers are usually the only machines that get backed up. Most companies do not back up individual users' machines. If your users place all their important documents in the home folder location on the network, those documents will get backed up as part of the nightly backup.

To specify a local 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. When connecting to a UNC name, the network folder you are connecting to 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 10 will attempt to create the folder for you. You can also use the variable %username% in place of a specific user's name. The %username% will automatically change to the name of the user you are currently working on.

> **WARNING** Be careful when you're specifying your home folder. If you make a mistake when typing in the path for the directory, Windows will create a bogus-named folder for you.

Complete Exercise 8.10 to assign a home folder to a user. These steps assume you have completed Exercises 8.2 onward.

EXERCISE 8.10

Assigning Home Folders

1. Open the Local Users and Groups MMC Desktop shortcut and expand the Local Users and Groups snap-in.

2. Open the Users folder and double-click user GWashington. The GWashington 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\GWashington** in the text box for the Local Path option. Then click OK.

5. Use Windows Explorer to verify that this folder was created.

6. Close the Local Users and Groups MMC.

🌐 **Real World Scenario**

Using Home Folders to Keep Files Backed Up

As an administrator for a large network, one of my 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 can also have 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 will 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 and store them 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:

1. Decide which server will store the users' home folders.

2. Create a directory structure that will store the home folders efficiently (for example, `C:\HOME`).

3. Create a single share to the user's home folder. (You can do this by right-clicking the home folder and choosing Properties.)

4. Use NTFS and share permissions to ensure that only the specified user has permissions to their home folder.

5. Specify the location of the home folder through the Profile tab of the user's Properties dialog box.

Troubleshooting User Account Authentication

When a user attempts to log on through Windows 10 and is unable to be authenticated, you will need to track down the reason for the problem.

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.

> **NOTE** Because many of these same issues happen when logging on to a domain from a Windows 10 machine, these approaches can be used for both local logons and domain logons.

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 10 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 by checking the account properties through the Local Users and Groups utility. If the account is no longer in the database, then it has most likely been deleted.

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 the user has chosen the correct option.

Managing and Creating 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 10 includes built-in local groups (such as Administrators and Backup Operators) that already have all the permissions needed to accomplish specific tasks. Windows 10 also uses built-in special groups in which users are placed automatically when they meet certain criteria.

You can create and manage local groups (but not special groups) through the Local Users and Groups utility. With this utility, you can add groups, change group membership, rename groups, and delete groups.

> **NOTE**
>
> One misconception about groups is that they have to work with Group Policy Objects (GPOs). This is not correct. Group Policy Objects are sets of rules that allow you to set computer-configuration and user-configuration options that apply to users or computers. Group Policies, on the other hand, are typically used with Active Directory and are applied as Group Policy Objects.

Using Built-In Groups

On a Windows 10 computer, built-in 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 10 system handles automatically. These groups are described in the following sections.

Built-in Local Groups

A local group is a group that is stored on the local computer's accounts database. You can add users to these groups and can manage the groups directly on a Windows 10 computer. By default, some the following local groups are created on Windows 10 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

I will briefly describe each group, its default permissions, and the users assigned to the group by default.

> **NOTE** 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 you want to be members of the group.

Administrators   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 filesystem, 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.

> **NOTE** 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.

Backup Operators   Members of the Backup Operators group have permissions to back up and restore the filesystem, even if the filesystem is NTFS and they have not been assigned permissions to access the filesystem. However, the members of Backup Operators can access the filesystem only through the Backup utility. To access the filesystem directly, Backup Operators must have explicit permissions assigned. There are no default members of the Backup Operators local group.

Cryptographic Operators   The Cryptographic Operators group has access to perform cryptographic operations on the computer. There are no default members of the Cryptographic Operators local group.

Distributed COM Users   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.

Event Log Readers   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.

Guests   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.

IIS_IUSRS   The IIS_IUSRS group is used by Internet Information Services (IIS). The NT AUTHORITY\IUSR user account (premade for IIS) is a member of the IIS_IUSRS group by default.

Network Configuration Operators   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.

Performance Log Users   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. There are no default members of this group.

Performance Monitor Users   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. There are no default members of this group.

Power Users   The Power Users group is included in Windows 10 for backward compatibility to ensure that computers upgraded from Windows XP function as before with regard to folders that allow access to members of the group. Otherwise, the Power Users group has limited administrative rights. There are no default members of this group.

Remote Desktop Users   The Remote Desktop Users group allows members of the group to log on remotely for the purpose of using the Remote Desktop service. There are no default members of this group.

Replicator   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.

Users   The Users group is intended for end users who should have very limited system access. If you have installed a fresh copy of Windows 10, 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.

Special Groups

Special groups are premade groups that can be used by the system or by administrators. Membership in special groups is automatic if certain criteria are met. You cannot manage special groups through the Local Users and Groups utility, but an administrator can add special groups to resources. The following text describes the special groups that are built into Windows 10.

Anonymous Logon   This group includes users who access the computer through anonymous logons. When users gain access through special accounts created for anonymous access to Windows 10 services, they become members of the Anonymous Logon group.

Authenticated Users   This group includes users who access the Windows 10 operating system through a valid username and password. Users who can log on belong to the Authenticated Users group.

Batch   This group includes users who log on as a user account that is used only to run a batch job.

Creator Owner   This is the account that created or took ownership of an 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.

Dialup   This group includes users who log on to the network from a dial-up connection.

Everyone   This group includes anyone who could possibly access the computer—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   This group includes all users who use the computer's resources locally.

Network   This group includes users who access the computer's resources over a network connection.

Service   This group 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.

System   There are times when the Windows 10 operating system will access functions within the system. When the operating system accesses these functions, it does it as a system user. When the system accesses specific functions as a user, that process becomes a member of the System group.

Terminal Server User   This group includes users who log on through Terminal Services.

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.

Keep your naming conventions in mind when assigning names to groups, just as you do when choosing usernames. Consider the following guidelines:

- The group name should be descriptive; for example, Accounting Data Users.
- The group name must be unique to the computer and 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 MMC or used Local Users and Groups through the Computer Management utility, 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 8.11.

FIGURE 8.11   The New Group dialog box
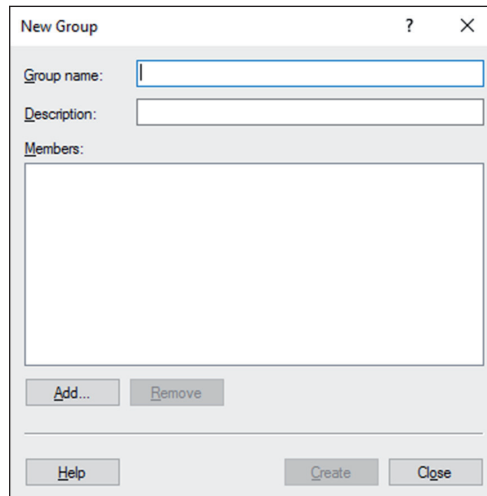
The only required entry in the New Group dialog box is the group name. If appropriate, you can enter a description for the group, and you can add (or remove) group members. When you're ready to create the new group, click the Create button.

Complete Exercise 8.11 to create two new local groups. (Creating domain groups is beyond the scope of this book.)

EXERCISE 8.11

Creating Local Groups

1. Open the Admin Console MMC Desktop shortcut you created 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. Repeat step 3, but type **Application Users** in the Group Name text box.

After the groups are created, you will have to manage the groups and their membership. In the next section, we will look at managing groups.

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 8.12. To access a group's Properties dialog box from the Groups folder in the Local Users and Groups utility, double-click the name of the group you want to manage.

FIGURE 8.12   Group's Properties dialog box
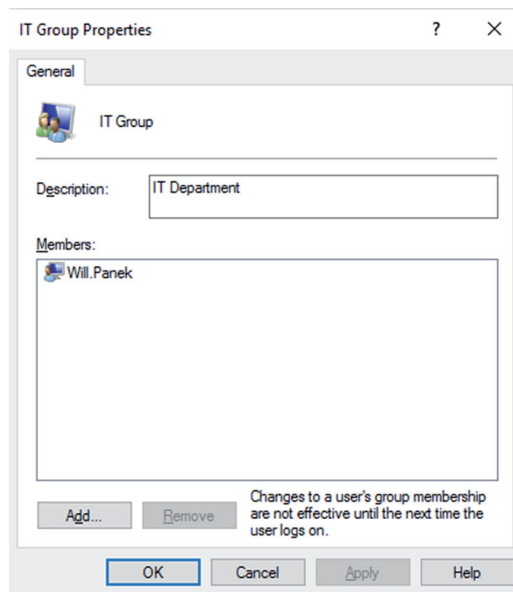
From the group's Properties dialog box, you can change the group's description and add or remove group members. When you click the Add button to add members, the Select Users dialog box appears (Figure 8.13).

FIGURE 8.13   The Select Users dialog box
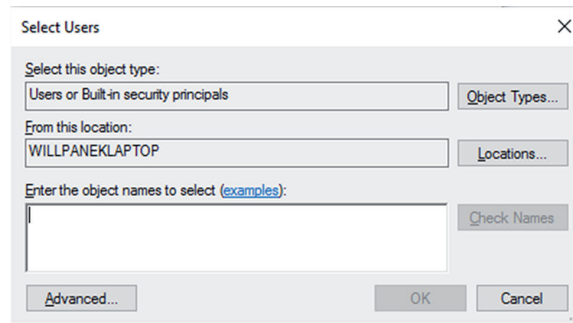
In the Select Users dialog box, you enter the object names of the users you want to add. You can use the Check Names button to validate the users against the database. Select the user accounts you wish to add and click Add. Click the OK button to add the selected users to the group.

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 8.12, you'll create new user accounts and then add these users to one of the groups you created in the previous steps.

EXERCISE 8.12

Adding Accounts to Groups

1. Open the Local Users and Groups MMC shortcut you created and expand the Local Users and Groups snap-in.

2. Create two new users: JDoe and DDoe. 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.

5. In the Data Users Properties dialog box, click the Add button.

6. In the Select Users dialog box, type the username **JDoe**; then click OK.

7. Click Add and type the username **DDoe**; then click OK.

8. In the Data Users Properties dialog box, you will see that the users have both been added to the group. Click OK to close the group's Properties dialog box.

There may come a point when a specific group is no longer needed. In the next section, we will look at how to delete a group from the Local Users and Groups utility.

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 name 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 because, like users, groups get unique SIDs assigned at the time of creation.

Creating users and groups is one of the most important tasks that we as IT members can do. On a Windows 10 machine, creating users and groups is an easy and straightforward process.

Now that you understand how to create users and groups, you need to know how to manage Windows 10 security using GPOs and LGPOs. We'll look at that next.

Managing Security Using GPOs and LGPOs

Windows 10 offers a wide variety of security options. If the Windows 10 computer is a part of a domain, then you can apply security through a Group Policy Object using the Group Policy Management Console. If the Windows 10 computer is not a part of a domain, then you use Local Group Policy Objects to manage local security.

Additionally, 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.

Understanding the GPO and LGPO Basics

The tools you use to manage Windows 10 computer security configurations depend on whether the Windows 10 computer is a part of a Windows 2000, Windows 2003, Windows 2008, Windows 2008/2008 R2, or Windows Server 2012/2012 R2 domain environment.

If the Windows 10 client is not a part of a domain, then you apply security settings through *Local Group Policy Objects (LGPOs).* LGPOs are sets of security configuration settings that are applied to users and computers. LGPOs are created and stored locally on the Windows 10 computer.

If your Windows 10 computer is a part of a domain, which uses the services of Active Directory, then you typically manage and configure security through Group Policy Objects (GPOs). Active Directory is the database that contains all your domain user and group accounts along with all other domain objects.

Group Policy Objects are policies that can be applied to either users or computers in the domain. The Group Policy Management Console (GPMC) is a Microsoft Management Console (MMC) snap-in that is used to configure and manage GPOs for users and computers via Active Directory.

Windows 10 computers that are part of a domain still have LGPOs, and you can use LGPOs in conjunction with the Active Directory group policies (GPOs).

> **NOTE** Usage of Group Policy Objects for domains is covered in greater detail in my book *MCSA Windows Server 2012 R2 Complete Study Guide: Exams 70-410, 70-411, 70-412, and 70-417* (Sybex, 2016).

The settings you can apply through the Group Policy utility within Active Directory are more comprehensive than the settings you can apply through LGPOs. Table 8.3 lists some of the options that can be set for GPOs within Active Directory and which of those options can be applied through LGPOs.

TABLE 8.3   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

Now that we have looked at LGPOs, let's look at some of the tools available for creating and managing them.

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 10 includes the Group Policy Result Tool, also known as the *Resultant Set of Policy (RSoP)*. You can access this tool through the GPResult command-line utility. The gpresult command displays the set of policies that were enforced on the computer and the specified user during the logon process.

The gpresult command will display the RSoP for the computer and user who is currently logged in. Several switches can be used with the gpresult command; Table 8.4 shows the different switches that can be used for the gpresult command.

TABLE 8.4 gpresult switches

Switch	Explanation
/F	Forces gpresult to override the filename specified in the /X or /H command
/H	Saves the report in an HTML format
/P	Specifies the password for a given user context
/R	Displays RSoP summary data
/S	Specifies the remote system to connect to
/U	Specifies the user context under which the command should be executed
/V	Specifies that verbose information should be displayed
/X	Saves the report in XML format
/Z	Specifies that the super-verbose information should be displayed
/?	Shows all the gpresult command switches
/scope	Specifies whether the user or the computer settings need to be displayed
/User	Specifies the username for which the RSoP data is to be displayed

In the next section, we will look at how to create and apply Local Group Policy Objects to the Windows 10 machine.

Managing and Applying LGPOs

Policies that have been linked through Active Directory will, by default, 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 does not use Active Directory.

Pre-Vista versions of Windows contained only one Local Group Policy Object that applied to all of the computer's users unless NTFS permissions were applied to the LGPO. However, Windows 10 and Windows Vista changed that with the addition of *Multiple Local Group Policy Objects (MLGPOs)*. MLGPOs are applied in the following 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 contain only user settings. Settings applied here will apply to all users of the computer.

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 included with Windows 10. These LGPOs make it possible for specific policy settings to apply to a single user.

As with Active Directory GPOs, any GPO settings applied lower in the hierarchy will override GPO settings applied higher in the hierarchy by default. 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.

> **NOTE**   Domain administrators can disable LGPOs on Windows 10 computers by enabling the Turn Off Local Group Policy Objects Processing Domain GPO setting under `Computer Configuration\Administrative Templates\ System\Group Policy`.

You apply an LGPO to a Windows 10 computer through the Group Policy Object Editor snap-in within the MMC. Figure 8.14 shows the Local Computer Policy for a Windows 10 computer.

FIGURE 8.14 Local Computer Policy
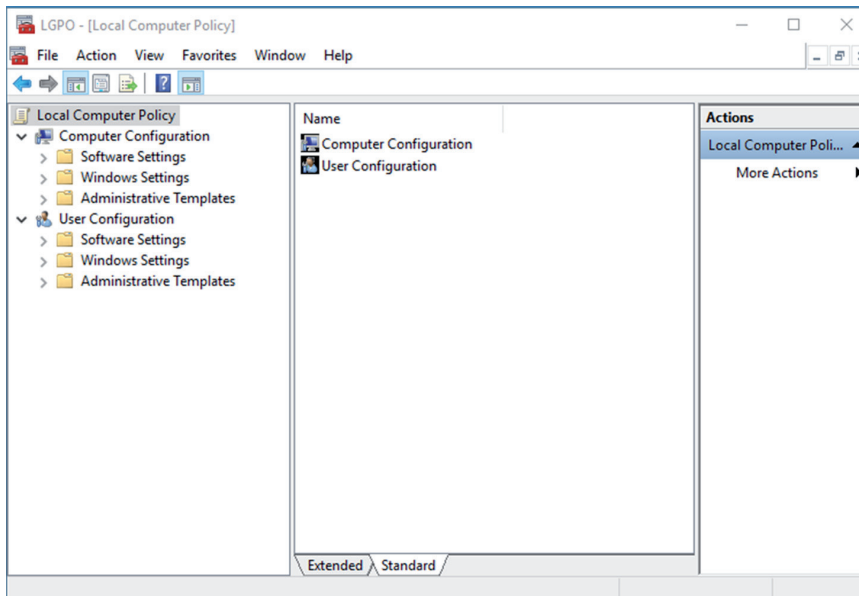
Complete Exercise 8.13 to add the Local Computer Policy snap-in to the MMC.

EXERCISE 8.13

Adding the Local Computer Policy Snap-In

1. Open the Local Users and Groups MMC shortcut by typing **MMC** in the Search Programs And Files box.

2. A User Account Control dialog box appears. Click Yes.

3. Select File ➢ Add/Remove Snap-in.

4. Highlight the Group Policy Object Editor snap-in and click the Add button.

5. The Group Policy Object specifies Local Computer by default. Click the Finish button.

6. In the Add Or Remove Snap-Ins dialog box, click OK.

7. In the left pane, right-click the Local Computer Policy and choose New Windows From Here.

8. Choose File ➢ Save As and name the console **LGPO**. Make sure you save it to the Desktop. Click Save.

9. Close the Local Users and Groups MMC.

Now we will look at how to open an LGPO for a specific user account on a Windows 10 machine. Complete Exercise 8.14 to access the Administrators, Non-Administrators, and User-Specific LGPOs.

EXERCISE 8.14

Accessing an LGPO

1. Open the Local Users and Groups MMC shortcut by typing **MMC** in the Windows 10 Search box.

2. Select File ➢ Add/Remove Snap-In.

3. Highlight the Group Policy Object Editor snap-in and click the Add button.

4. Click Browse so that you can browse for a different GPO.

5. Click the Users tab.

6. Select the user 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 have finished looking at the LGPO settings for the user you chose.

> **NOTE**   Notice that the Administrators, Non-Administrators, and User-Specific LGPOs contain only User Configuration settings, not Computer Configuration settings.

Now let's take a look at the different security settings that can be configured in the LGPO.

Configuring Local Security Policies

Through the use of 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 main areas of security configuration of the LGPO are as follows:

Account Policies   Account policies are used to configure password and account lockout features. Some of these settings include password history, maximum password age, minimum password age, minimum password length, password complexity, account lockout duration, account lockout threshold, and whether to reset the account lockout counter afterward.

Local Policies   Local policies are used to configure auditing, user rights, and security options.

Windows Firewall with Advanced Security   Windows Firewall with Advanced Security provides network security for Windows computers. Through this LGPO, you can set domain, private, and public profiles. You can also set this LGPO to authenticate communications between computers and inbound/outbound rules.

Network List Manager Policies   This section allows you to set the network name, icon, and location group policies. Administrators can set Unidentified Networks, Identifying Networks, and All Networks.

Public Key Policies   Use the Public Key Policies settings to specify how to manage certificates and certificate life cycles.

Software Restriction Policies   The settings under Software Restriction Policies allow you to identify malicious software and control that software's ability to run on the Windows 10 machine. These policies allow an administrator to protect the Microsoft Windows 10 operating system against security threats such as viruses and Trojan horse programs.

Application Control Policies   This section allows you to set up AppLocker. You can use AppLocker to configure a Denied list and an Accepted list for applications. Applications that are configured on the Denied list will not run on the system, and applications on the Accepted list will operate properly.

IP Security Policies on Local Computer   This section allows you to configure the IPsec policies. IPsec is a way to secure data packets at the IP level of the message.

Advanced Audit Policy Configuration   Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies. This section also allows you to configure auditing to help show administrators either successful or unsuccessful attacks on their network.

> **NOTE**   You can also access the Local Security Policy by running `secpol.msc` or by opening Control Panel and selecting Administrative Tools ➢ Local Security Policy.

Now that you have seen all the options in the security section of the LGPO, let's take a look at account policies and local policies in more detail.

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 10 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.

> **NOTE**   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 need to 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. 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 password policies are set on a per-computer basis; they cannot be configured for specific users. Figure 8.15 shows the password policies, which are described in Table 8.5.

FIGURE 8.15   The password policies
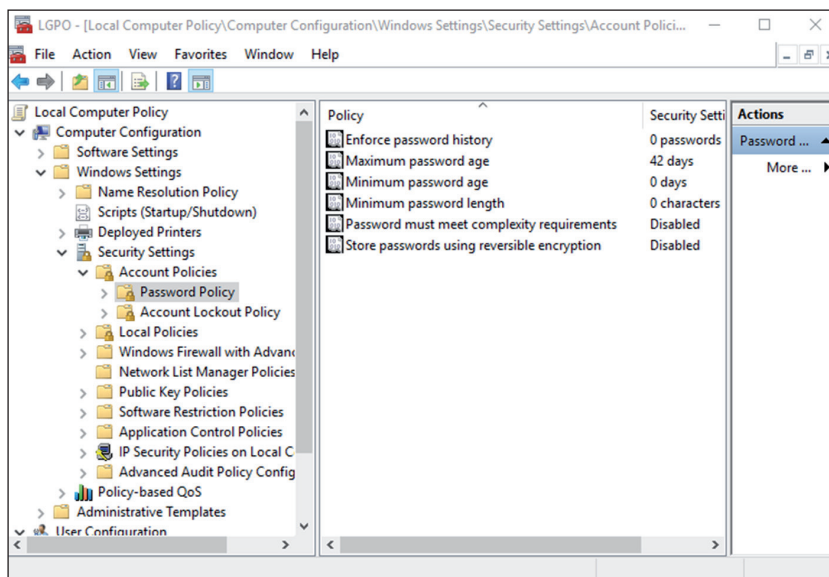
TABLE 8.5 Password policy options

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	No minimum	No maximum
Store Passwords Using Reversible Encryption	Specifies higher level of encryption for stored user passwords	Disabled	No minimum	No maximum

You can use the password policies in Table 8.5 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 passwords 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 passwords several times in rapid succession in order to defeat the purpose of the Enforce Password History policy.

Minimum Password Length   Ensures that a user creates 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 four 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).

Complete Exercise 8.15 to configure password policies for your computer. These steps assume that you have added the Local Computer Policy snap-in to the MMC in Exercise 8.1.

EXERCISE 8.15

Configuring Password Policy

1. Open the LGPO MMC shortcut that you created earlier.

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 five 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.

Let's now look at how to set and manage the policies in the Account Lockout Policies section.

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 it.

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 8.16 shows the account-lockout policies, which are described in Table 8.6.

FIGURE 8.16 Account-lockout policies
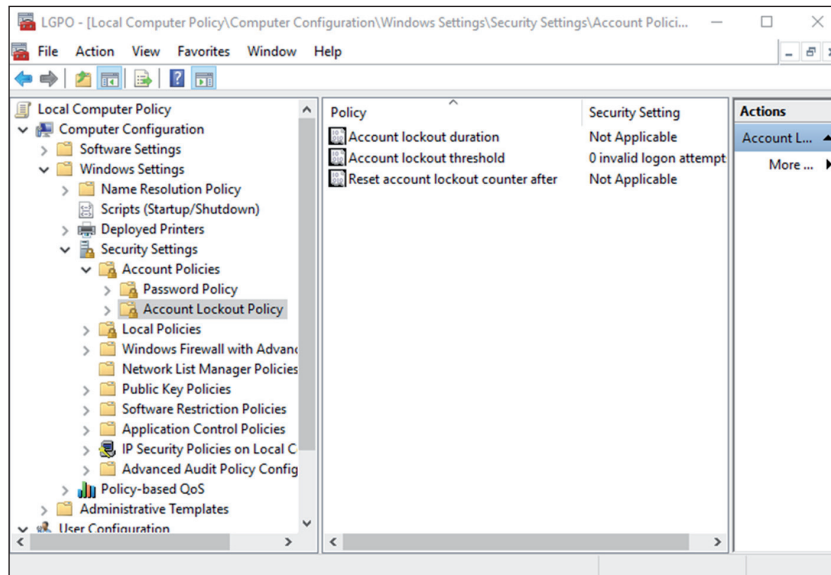
TABLE 8.6 Account-lockout policy options

Policy	Description	Default	Minimum	Maximum
Account Lockout Duration	Specifies how long account will remain locked if the account lockout threshold is reached	Disabled (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 (If Account Lockout Threshold is enabled, 30 minutes.)	Same as default; if enabled, must be equal to or less than the Account Lockout Duration value.	99,999 minutes

The Account Lockout Duration and Reset Account Lockout Counter After policies will be disabled until a value is specified for the Account Lockout Threshold policy. After the Account Lockout Threshold policy is set, the Account Lockout Duration and Reset Account Lockout Counter After policies will be set to 30 minutes. If you set Account Lockout Duration to 0, the account will remain locked out until an administrator unlocks it.

> **NOTE**
>
> The Reset Account Lockout Counter After value must be equal to or less than the Account Lockout Duration value.

Complete Exercise 8.16 to configure account-lockout policies and test their effects.

EXERCISE 8.16

Configuring Account-Lockout Policies

1. Open the LGPO MMC shortcut.

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 Account Lockout Threshold policy. On the Local Security Setting tab, specify that the account will lock after three 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 one of the accounts that have been created on this Windows 10 machine and enter 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 the account, open the Local Users and Groups snap-in in the MMC, expand the `Users` folder, and double-click the user.

11. On the General tab of the user's Properties dialog box, click to remove the check mark 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 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. 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 8.17 shows the three Local Policies folders: Audit Policy, User Rights Assignment, and Security Options. We will look at Audit Policy and User Rights Assignment in the following sections.

FIGURE 8.17 Accessing the Local Policies folders
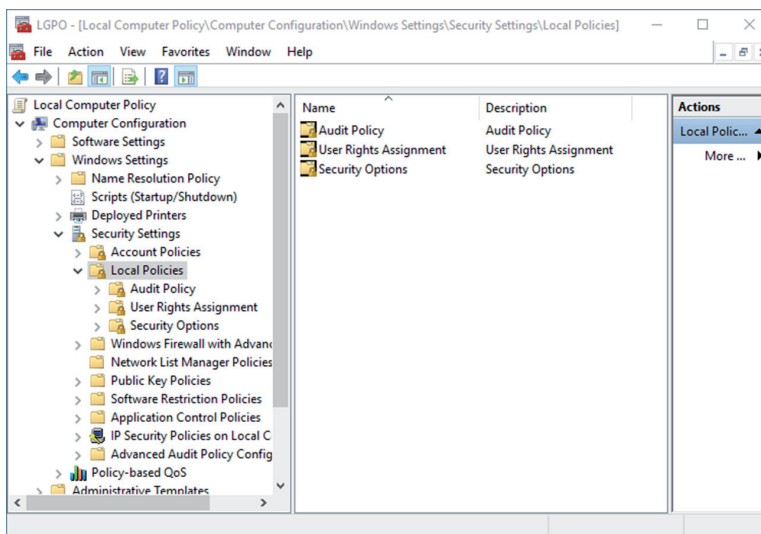
Setting Audit Policies

Audit policies can be implemented to track the 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.

🌐 Real World Scenario

Auditing Failed Attempts

As an IT manager, you have to make sure that you monitor failed attempts to access resources. A failed attempt to access a resource usually means that someone tried to access the resource and was denied because of insufficient privileges.

> 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.
>
> If a user is trying to access an area in which they do not belong, make sure to warn the user. This is very common on a network and needs to be nipped in the bud.

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.

> **NOTE**   Only members of the Administrators group can view the security log in Event Viewer.

Figure 8.18 shows the audit policies, which are described in Table 8.7.

FIGURE 8.18   Audit policies
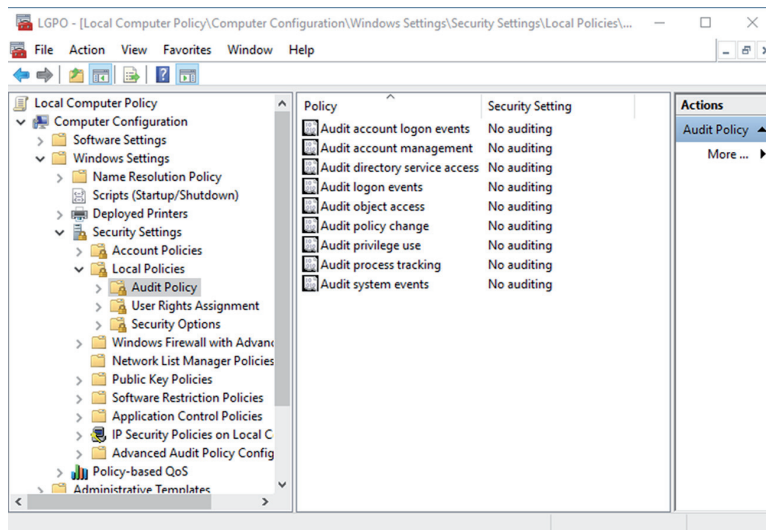
After you set the Audit Object Access policy to enable auditing of object access in the object's properties, you must enable file auditing through NTFS security or print auditing through printer security.

Complete Exercise 8.17 to configure audit policies and view their results.

EXERCISE 8.17

Configuring Audit Policies

1. Open the LGPO MMC shortcut.

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 Success and Failure boxes. Click OK.

5. Open the Audit Account Management policy. Check the Success and Failure boxes. Click OK.

6. Log off of your Administrator account. Attempt to log back on to your Administrator account using an incorrect password. The logon should fail (because the password is incorrect).

7. Log on as an administrator.

8. Select Start, right-click Computer, and choose Manage 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.

TABLE 8.7   Audit-policy options

Policy	Description
Audit Account Logon Events	Tracks when a user logs on or logs off either their local machine or the domain (if domain auditing is enabled).
Audit Account Management	Tracks user and group account creation, deletion, and management actions, such as password changes.
Audit Directory Service Access	Tracks directory service accesses.
Audit Logon Events	Audits events related to logon, such as running a logon script, accessing a roaming profile, and accessing a server.
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.

Assigning User Rights

The user-rights policies determine what rights a user or group has on the computer. User rights, also called privileges, apply to the system. They are not the same as permissions, which apply to a specific object. An example of a user right is Back Up Files And Directories. 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 filesystem permissions. The other user rights are similar because they deal with system access as opposed to resource access.

Figure 8.19 shows the first several user-rights policies; all of the policies are described in Table 8.8.

FIGURE 8.19   User-rights policies
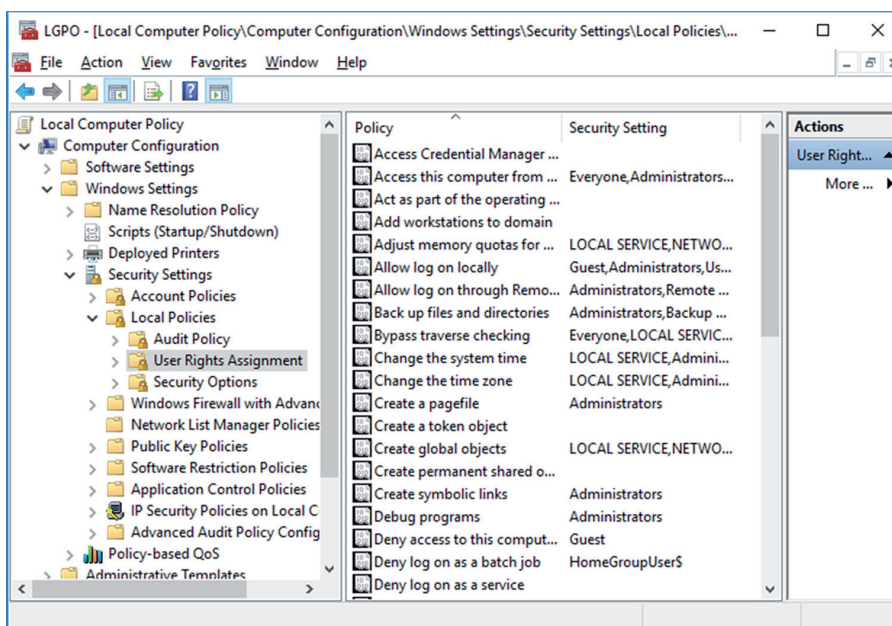
In Exercise 8.18, you'll apply a user-rights policy.

TABLE 8.8   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.

TABLE 8.8 User Rights Assignment policy options *(continued)*

Right	Description
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.
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 Remote Desktop Services	Gives a user permission to log on through Remote Desktop Services.
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 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.

Right	Description
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.
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.
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. A user or computer that is trusted for delegation can access resources on another computer using delegated credentials of a client.
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	The working set of a process is the current set of pages in the virtual address space of the process that resides in physical memory. This setting allows you to increase the size of the process working set.
Increase Scheduling Priority	Specifies that a process can increase or decrease the priority that is assigned to another process.

TABLE 8.8   User Rights Assignment policy options *(continued)*

Right	Description
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.
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.
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 10 user interface.
Replace A Process Level Token	Allows a process, such as Task Scheduler, to call an API to start another service.

Right	Description
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 10 computer locally.
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.

EXERCISE 8.18

Applying a User-Rights Policy

1. Open the LGPO MMC shortcut.

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 a user. 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.

Configuring 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 able to perform administrative functions.

The problem is that many applications require that users have permissions to write to protected folders and to the Registry. Windows 10's solution 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 administrative tasks 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 security shield. For example, the small shield shown on the Change Date And Time button in the Date And Time dialog box indicates an action that requires privilege elevation.

Now let's take a look at how to elevate privileges for users and executables.

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. This 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. The UAC does this automatically. If you do not want standard users to be prompted at all for credentials when attempting to perform administrative tasks, you change 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 built-in 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.

> With the Default UAC setting enabled, a user's desktop will be dimmed when they are notified of a change to the computer. The administrator or user must either approve or deny the request in the UAC dialog box before the user can do anything else on that computer. This is known as the *secure desktop*. You have the ability to turn off the secure desktop by modifying either the Local Security Policy or the Registry.

Complete Exercise 8.19 to see how UAC affects administrator and non-administrator accounts differently.

EXERCISE 8.19

Seeing How UAC Affects Accounts

1. Log on to Windows 10 as a non-administrator account.

2. Right-click Start ➤ Control Panel ➤ Large Icons View ➤ Windows Firewall.

3. Click the Turn Windows Firewall On Or Off link on the left side. The UAC box should prompt you for permission to continue. Click Yes. You should be denied access to the Windows Firewall Settings dialog box.

4. In the Users and Groups MMC, enable the Administrator account and also reset the Administrator's password.

5. Log off and log on as the Administrator account.

6. Right-click Start ➤ Control Panel ➤ *Large Icons View* ➤ Windows Firewall.

7. Click the Turn Windows Firewall On Or Off link.

8. You should automatically be taken to the Windows Firewall screen. Close the Windows Firewall screen.

Let's now take a look at elevating privileges for executable applications.

Elevated Privileges for Executables

You can also enable an executable file to run with elevated privileges. To do so, you can right-click a shortcut or executable and select Run As Administrator. The elevation applies to this session only.

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 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

because the program doesn't need administrative privileges or you are not logged on as an administrator.

Registry and File Virtualization

Many applications that are installed on a Windows 10 machine need to have access to the Registry. By default, Windows 10 protects the Registry from non-administrator accounts, but a feature called Registry and File Virtualization enables 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 10 redirects any attempts to write to protected locations to a per-user location. By doing so, Windows 10 enables users to use the application successfully while it protects critical areas of the system.

Understanding Smart Cards

Another way to help secure Windows 10 is by using smart cards. *Smart cards* are plastic cards (the size of a credit card) that can be used in combination with other methods of authentication. This process of using a smart card along with another authentication method is called two-factor authentication or *multi-factor authentication*. Authentication is the process of using user credentials to log on to either the local Windows 10 machine or the domain.

Multi-factor authentication support allows you to increase the security of many critical functions of your company, including client authentication, interactive logon, and document signing.

Multi-factor authentication (using smart cards) is now easier than ever to use and deploy because of the new features included with all versions of Windows 10.

Enhanced Support for Smart Card–Related Plug and Play and the Personal Identity Verification (PIV) Standard   This allows users of Windows 10 to use smart cards from vendors who publish their drivers through Windows Update, allowing Windows 10 to use the smart card without special middleware. These drivers are downloaded in the same way as drivers for other Windows devices. When a smart card that is PIV-compliant is placed into a smart-card reader, Windows 10 will try to download a current driver from Windows Update. If a driver is not available, the PIV-compliant minidriver that is included with Windows 10 is used for the smart card.

Encrypting Drives with BitLocker   If your users are using Windows 10 Enterprise or Professional, the users can choose to encrypt their removable media by turning on BitLocker and then choosing the smart-card option to unlock the drive. Windows will then retrieve the correct minidriver for the smart card and allow the operation to complete.

Smart-Card Domain Logon   When using Windows 10, the correct minidriver for a smart card is automatically retrieved. This allows a new smart card to authenticate with the domain controller without requiring the user to install or configure additional middleware.

Document and Email Signing   Windows 10 users can use smart cards to sign an email or document. XML Paper Specification (XPS) documents can also be signed without additional software.

Use with Line-of-Business Applications   Using Windows 10 smart cards allows applications that use Cryptography Next Generation (CNG) or CryptoAPI to retrieve the correct minidriver at runtime. This eliminates the need for middleware.

When you decide to use multi-factor authentication, you are deciding to use a process that will require certificate authorities (CAs). CAs are servers that are running the certificate services on them. When you move forward with the decision to use smart cards, you will then need to install and configure CAs to make all of the components work together.

CAs are built on Windows Server operating systems, and if your Windows 10 users are having issues logging into the Windows 10 operating systems using smart cards, then you must check the server CAs to make sure that they are configured and running properly.

> **NOTE**   Certificate Servers are covered in greater detail in *MCSA Windows Server 2012 R2 Complete Study Guide: Exams 70-410, 70-411, 70-412, and 70-417* by William Panek (Sybex, 2016).

There are two types of smart cards: physical and virtual. Physical smart cards are cards that look like ATM cards. Most of them have either a magnetic strip or chip built into the physical card. To use a physical smart card, you need a smart card reader. This is a device that either connects to a computer or is built into a computer and you place the physical smart card into the reader. You then enter a PIN into the system and the machine is unlocked or logged into the network.

There is a downside to using physical smart cards, which is that they can get lost or misplaced. When I implemented a smart card system into a previous company, we ended up replacing one-fourth of all cards in the first month due to loss or damage.

This is where virtual smart cards can be an advantage. Virtual smart cards use a cryptographic key technology that is stored on the actual Windows 10 computer, as long as that computer has a Trusted Platform Module (TPM) installed on the motherboard.

Virtual smart cards offer the security benefits of two-factor authentication without the price of physical cards and readers. This is possible because of the TPM technology. TPM devices allow us to use cryptographic capabilities, the same as physical smart cards do, but without the cards. Virtual smart cards give us the same benefits as physical cards, including non-exportability, anti-hammering, and isolated cryptography.

Non-exportability   TPM technology is built to be tamper proof. When a system uses TPM encryption, the TPM encryption is specific to the machine that installed it. Because of this, you can't take a virtual smart card from one system and use it on another.

Anti-hammering (Lockout)   Smart cards use PINs to unlock the system. If a PIN is entered incorrectly, the TPM uses an Anti-hammering technology that locks the system from further attempts for a specific amount of time.

Isolated Cryptography   TPMs are the only mechanism on a Windows 10 system that loads a copy of the private keys. These keys are not loaded into the system's memory, and because only TPM has the keys, the keys stay isolated and inaccessible to anything or anyone.

Virtual smart cards function the same way as physical smart cards that are continuously inserted into a system. The machine gets the same benefits and results. To set up virtual smart cards, you need to build a certificate authority (CA) server in your organization, and all of your Windows clients need to be Windows 8 or higher.

After the CA is built, you then need to build a certificate template for the virtual smart cards to use. Then, to create the TPM virtual smart card for a Windows 10 system, open a command prompt with Administrative credentials on a Windows 10 domain computer and type in the following command:

```
tpmvscmgr.exe create /name tpmvsc /pin default /adminkey random /generate
```

After you run this command, you will create a virtual smart card with the name `tpmvsc`. The system will then prompt you for a PIN. You will need to enter and confirm a PIN of at least eight characters. After a few seconds, the process will complete. The TPM application (`tpmvscmgr.exe`) will then provide you with the device instance ID for the virtual smart card. You may want to store this ID in case you will need it to manage or remove the virtual smart card later.

Finally, you will need to enroll the certificate into the CA by requesting a new certificate and then choosing the TPM Virtual Smart Card Logon check box. When you are prompted for a device, select the Microsoft virtual smart card that you created earlier.

Summary

In this chapter, you learned how to create and manage user and group accounts. We looked at the different tools that can be used to create users in Windows 10.

We also looked at Windows 10 security. We reviewed the difference between LGPOs, which are applied at the local computer level, and GPOs, which are applied through a Windows 2003, 2008, 2008 R2, or 2012/2012 R2 domain, and how they are applied.

We looked at account policies, which control the logon process. The two types of account policies are password and account lockout policies. We also looked at 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.

Video Resources

There are videos available for the following exercises:

8.1

8.3

8.4

You can access the videos at `www.wiley.com/go/sybextestprep` on the Other Study Tools tab.

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.

Know how to manage local groups.   Understand the local groups that are created on Windows 10 computers by default, and be familiar with the rights each group has. Know how to create and manage new groups.

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.

Understand 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.

Review Questions

1. You are the administrator for a large training company. You have decided that everyone needs to configure the Password Must Meet Complexity Requirements policy. Users are not sure what they can use. You decide to send an email out showing people examples of what types of passwords they can use. Which of the following passwords meet the minimum complexity requirements? (Choose all that apply.)

   A. aBcdEfG1!

   B. Abc-de!

   C. Kl982!@#$%^&*

   D. 123456789nA

2. You are setting up a machine for a home user who does not know much about computers. You do not want to make the user a local administrator, but you do want to give this user the right to change Windows Updates manually. How can you configure this?

   A. Modify the LGPO for Windows Update to allow the user to make changes manually.

   B. Explain to the user how to log on as the Administrator account.

   C. Set Windows Update modifications to anyone.

   D. This can't be done. Only administrators can change Windows Update.

3. You are the administrator for a large organization with multiple Windows Server 2012 R2 domain controllers and multiple domains. You have a Windows 10 machine that is set up for all users to access. You have an application called `StellApp.exe` that everyone on this Windows 10 computer can use except for the Sales group. How do you stop the Sales group from accessing this one application?

   A. Deny the Everyone group the rights to the application.

   B. Create an executable rule from the Application Control Policy.

   C. Create a security role from the Application Control Policy.

   D. Give the Everyone group full control to the application.

4. You have a Windows 10 machine that multiple users access. All users have the rights to use USB removable devices, but you need to deny one user access to USB removable devices. How do you accomplish this?

   A. Deny the one user from using the machine.

   B. Set a USB rule on Hardware Manager.

   C. Deny all users from using USB devices.

   D. Create a removable storage access policy through an LGPO.

5. You are the system administrator for a large organization. You have a Windows 10 machine that all users can access. There is a folder on the Windows 10 machine called `Apps`. You need to set up auditing on this folder. How do you accomplish this task?

   A. From the Local Group Policy, enable Directory Service Access.

   B. From the Local Group Policy, enable Audit Object Access.

    C. From the Local Group Policy, enable Account Access.

    D. From the Local Group Policy, enable File And Folder Access.

6. Your company, Stormwind, requires that you implement security and you have been asked to define and implement a security policy. You have configured password policies so that users must change their passwords every month. Users are not allowed to use any of their previous 24 passwords. Which password policy would you implement if you want to prevent users from reusing passwords?

    A. Passwords Must Be Advanced

    B. Enforce Password History

    C. Passwords Must Be Unique

    D. Passwords Must Meet Complexity Requirements

7. You are the network administrator for a large organization. You have a Windows 10 machine that needs to prevent any user from copying unencrypted files from the Windows 10 machine to any removable disk. How do you accomplish this task?

    A. Within the System icon in Control Panel, set the BitLocker Drive Encryption.

    B. Within the Hardware icon in Control Panel, set the BitLocker Drive Encryption.

    C. Within the Device Manager icon in Control Panel, set the BitLocker Drive Encryption.

    D. Within a Local Group Policy, set the BitLocker Drive Encryption.

8. In which editions of Windows 10 can you enable UAC? (Choose all that apply.)

    A. Windows 10 Home edition

    B. Windows 10 Education edition

    C. Windows 10 Professional edition

    D. Windows 10 Enterprise edition

9. A salesperson in your company purchases a new laptop with Windows 10 installed. She asks you to configure it for her. You create a standard local user account for her. Which of the following tasks can she perform by default?

    A. Change date and time settings

    B. Change time-zone settings

    C. Check Device Manager

    D. Enable parental controls

10. 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 Policy box should you define?

    A. Password Policy

    B. Account Lockout Policy

    C. Audit Policy

    D. Security Options

Chapter

9

Configuring Network Connectivity

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Configure IP settings.**

- This objective may include but is not limited to the following subobjectives: Configure name resolution, connect to a network, configure network locations.

✓ **Configure networking settings.**

- This objective may include but is not limited to the following subobjectives: Connect to a wireless network, manage preferred wireless networks, configure network adapters, configure location-aware printing.

✓ **Configure and maintain network security.**

- This objective may include but is not limited to the following subobjectives: Configure Windows Firewall, configure Windows Firewall with Advanced Security, configure connection security rules (IPsec), configure authenticated exceptions, configure network discovery.

In most organizations, Windows 10 machines will be configured as a member of a domain. Therefore, it's very important to know how to properly configure Windows 10 in a domain environment.

In this chapter, we discuss Active Directory and how to configure Windows 10 to work within the Windows Server 2012 R2 domain environment. We will look at how to connect to a Windows Server 2012 R2 domain by using both IPv4 and IPv6. We will also look at connecting Windows 10 to a network by using either a wireless or wired connection and working with the Windows 10 HomeGroup.

We will look at how to protect your network by using the Windows 10 Firewall. We discuss the different ways that you can manage your network and Windows 10 machines remotely.

Another technology that we present in this chapter is virtualization. This is one of the fastest growing and hottest technologies to hit the market in the past few years. Server virtualization gives an organization the ability to run multiple operating systems, called *virtual machines*, on a single physical machine. We will look at how to install and configure Windows 10 to run as a virtual machine.

Understanding Networking

Microsoft uses two networking models: domain-based networks and peer-to-peer networks. The way you design your network is going to determine how you set up the rest of the computers and servers on that network. The choice you make here will be determined by many factors, including the number of users on your network and the amount of money you can spend.

Windows Peer-to-Peer Network

When setting up a Microsoft Windows *peer-to-peer network* (also referred to as a *workgroup*), it is important to understand that all computers on the network are equal. All of the peer-to-peer computers, also referred to as *nodes*, simultaneously act as both clients and servers.

Peer-to-peer networks are typically any combination of Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, and Windows 10 machines connected by a centralized device such as a router or hub (see Figure 9.1).

FIGURE 9.1   Peer-to-peer model
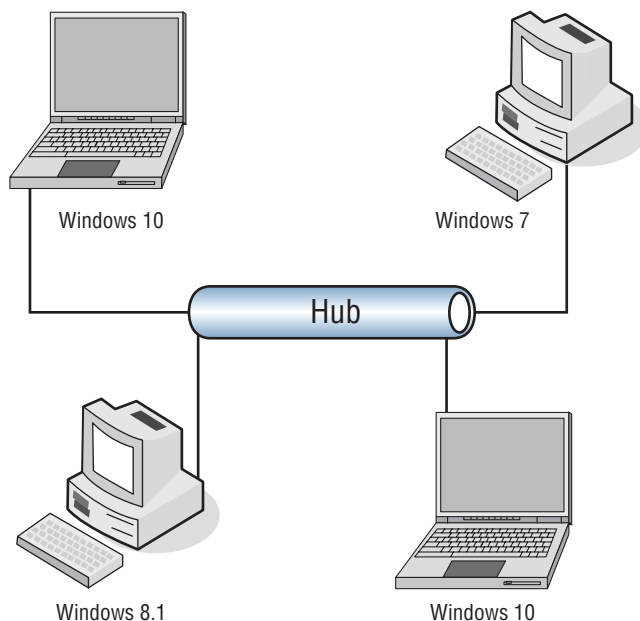
One of the biggest debates among IT professionals is when to use a peer-to-peer network. These types of networks have their place in the networking world. Most home networks use this type of configuration—where all of the computers are connected by a small Internet router. It's often the same for companies. You would use this network configuration in a small environment with 10 users or fewer. This enables small organizations to still share resources without needing expensive equipment, server software, or an internal IT department.

But there is a downside to peer-to-peer networks; the biggest issue is manageability and security. Many new IT people like working on a small peer-to-peer network because of its size, but no matter what, a network with 10 users and 10 computers can be very difficult to manage and security is extremely difficult to set up. Because there is no server to centralize user accounts on a peer-to-peer network, each Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, and Windows 10 computer must have a user account and password. So if you have 10 users and 10 computers and all 10 users must be able to access all 10 computers, you end up creating 100 accounts: 10 accounts on each machine times 10 machines.

Another disadvantage of peer-to-peer networks is backups. Most IT departments do not back up individual user machines, and because there is no centralized server for data storage when using a peer-to-peer network, data recoverability can be an issue.

Now that you have seen the advantages and disadvantages of a peer-to-peer network, let's discuss the advantages and disadvantages of a domain-based network.

Windows Server 2012 R2 Active Directory Network

A *domain-based network* uses Microsoft's *Active Directory*, which is a single distributed database that contains all the objects in your network. A domain is a logical grouping of objects into a distributed database. Some of these objects are user accounts, group accounts, and published objects (folders and printers).

The first of many advantages to Active Directory is centralized management. As just stated, the Active Directory database contains all the network information within a single, distributed, data repository. Because these network objects are all located in the same database, an administrator can easily manage the domain from one location.

Another major advantage to using Active Directory is domain security. An administrator has the advantage of creating a single username and password for all users within the domain. This username and password can be used to access all resources that an individual has the proper rights to access. An administrator can determine, based on job function or position, which files or folders on the network a user should be granted access to, and assign access to the user's single account. In our earlier peer-to-peer example, you needed to create 100 user accounts. With a domain, you would need to create only the 10 accounts, one per person.

An Active Directory structure is made up of one or more domains. As explained, a *domain* is a logical grouping of objects within your organization. For example, if we had the Stormwind.com domain, all users in that domain should be members of the Stormwind.com organization. The objects that are contained within a domain do not need to be in the same physical location. Domains can span the entire globe even though they are part of the same organization.

One of the advantages to using domains is the ability to have a *child domain*, which is a subdomain of another domain. You can build child domains based on physical locations, departments, and so forth. Figure 9.2 shows the hierarchy structure of Stormwind.com with its child domains (based on geographic location).

> Microsoft Active Directory domains are represented as triangles. It is important to remember that when taking any Microsoft exam.

FIGURE 9.2   Domain structure
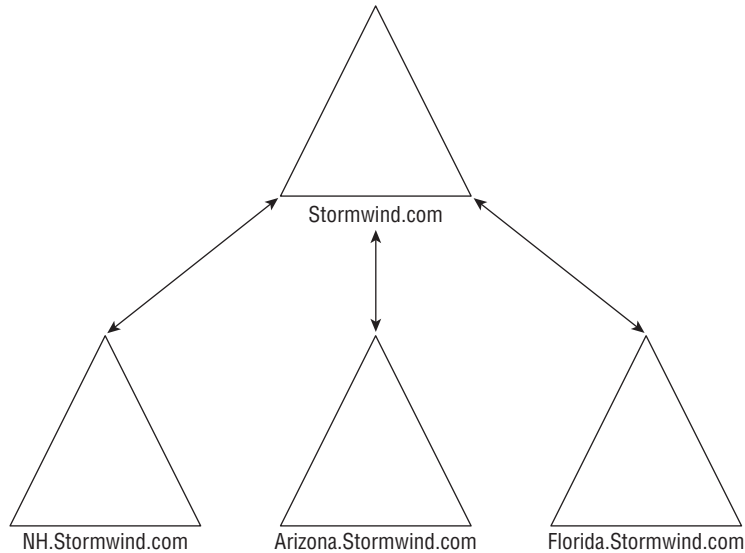
Child domains give you greater scalability. Active Directory has the ability to store millions of objects within a single domain, but child domains give an administrator the flexibility to design a structure that meets an organization's needs. For example, you may have a site located in a different state. Creating a child domain for that office allows that office to be an independent domain, and thus they can have their own security and domain settings. One or more domains that follow the same contiguous namespace are called a tree. For example, if my domain name is `Stormwind.com` and the child domains are `NH.Stormwind.com`, `Arizona.Stormwind.com`, and `Florida.Stormwind.com`, this would be a tree. All of these domains follow the `Stormwind.com` namespace.

When you set up child domains, the parent and child domains automatically establish a trust relationship. *Trusts* allow users to be granted access to resources in a domain even when their accounts reside in a different domain. To make administration of trust relationships easier, Microsoft has made transitive two-way trusts the default relationship between domains within a forest. A forest is all the trees that are part of your Active Directory structure, and they share a schema and Global Catalog. This means that by default, all domains within the same forest automatically trust one another. As shown in Figure 9.2, Stormwind.com automatically trusts NH.Stormwind.com, Arizona.Stormwind.com, and Florida.Stormwind.com. This means that all of the child domains implicitly trust one another.

The last Active Directory advantage that we will discuss is an extensible schema. The Active Directory schema contains all the objects and attributes of the database. For

example, when you create a new user by using the Active Directory Users and Computers snap-in, the system asks you to fill in the user's first name, last name, username, password, and so forth. These fields are the attributes of the user object, and the way that the system knows to prompt for these fields is that the user object has these specific attributes assigned to it within the Active Directory schema. An administrator has the ability to change or expand these fields based on organizational needs.

🌐 **Real World Scenario**

Extending the Schema

You may be asking yourself why an organization would need to extend the schema. Many years ago, when I got out of the military and before I got into the computer industry, I used to cast toilets for American Standard. I made 50 toilets a day. When working for American Standard, I had an employee number of 343. All my toilets were stamped 343 (so the company knew who made the product) on the base of the toilet. My time card did not even have my name, just my number.

This number is an example of a field that would need to be added to a schema. I would have an account in Active Directory with my name, but there would need to be a field that showed my employee number. You may have to adjust your Active Directory schema based on your organization's requirements.

The major disadvantage to an Active Directory model is cost. When setting up an Active Directory domain, an organization needs a machine that's powerful enough to handle the Windows Server 2012 R2 operating system. Also, most companies that decide to use a domain-based organization will require the IT personnel to manage and maintain the network infrastructure.

Cloud-Based Azure Active Directory

Now that you have been introduced to Active Directory, let's take a look at how you can have Microsoft manage your Active Directory with their cloud-based Active Directory called *Azure*. Azure is Microsoft's subscription-based Active Directory.

If you are a small- to mid-size company and you don't want to worry about employing a full-time multi-person IT department, then this may be a great option for you. This allows Microsoft to deal with the worries of managing and maintaining a server room and all of the hardware.

All your company would need to do is hire or train someone who would add and maintain the actual Azure Active Directory accounts. This person could also work as the help desk or support individual. Now you have Microsoft worrying about the hardware and your IT people can focus on helping and maintaining users and accounts.

So how does Azure Active Directory compare when it comes to adding Windows 10 to the domain? It really doesn't matter. As long as you have Internet access to the cloud-based system, your Windows 10 accounts will work the same way as if the Active Directory was on premise.

Windows 10 includes a new feature for configuring and deploying corporation-owned Windows devices called Azure AD Join. Azure AD Join registers the Windows 10 devices in the Azure Active Directory, which then allows them to be accessible and managed by your organization.

The one nice advantage is that with Azure Active Directory, Windows 10 devices authenticate directly to Azure AD without the need of an onsite domain controller. But, if you want, you can still have a domain controller on site that works with the cloud-based Azure Active Directory.

When you are adding Windows 10 to Azure Active Directory, end-users or domain admins can join their Windows 10 device (computer, tablet, or phone) to Azure AD during the out-of-box experience (OOBE). Because of this, organizations can assign devices to their users with no IT interaction or staging time.

Because of the Azure AD Join built into Windows 10, during the OOBE, the IT department would just add the device to the Azure Active Directory network.

Now that you understand the difference between a workgroup and a domain, let's go ahead and make sure that you understand some of the other networking terms that you will need to know.

Other Microsoft Networking Terms and Roles

Now that you have seen the different Microsoft networking models, let's talk about some of the server terminology that is used in the remainder of this chapter. You may be familiar with some of these terms, but it's always good to get a refresher.

Server   A *server* is a machine that users connect to so they can access resources located on that machine. These resources can be files, printers, applications, and so forth. Usually, the type of server is dependent on the resource that the user needs. For example, a print server is a server that controls printers. A file server contains files. Application servers can run applications for the users. Sometimes you will hear a server referred to by the specific application that it may be running. For example, someone may say, "That's our SQL server" or "We have an Exchange server."

Domain Controller   This is a server that contains a replica of the Active Directory database. As mentioned earlier in this chapter, Active Directory is the database that contains all the security objects in your network along with any resources that you publish to Active Directory. A *domain controller* is a server that contains this database. All domain controllers are equal in a Windows Server 2012 R2 network, and each can read from and write to the directory database. Some domain controllers may contain extra roles, but they all part of the same Active Directory.

Member Server   A *member server* is a server that is a member of a domain-based network but does not contain a copy of Active Directory. For example, it is recommended by Microsoft that a Microsoft Exchange server be loaded on a member server instead of a domain controller. Both domain controllers and member servers can act as file, print, or application servers. Your choice of server type depends on whether you need that server to have a replica of Active Directory.

Network Discovery   *Network discovery* is a setting that determines whether your Windows 10 system can locate other computers and devices on the network and if other computers on the network can see your computer. To enable or disable Network Discovery, you need to complete the following steps:

1. In the Windows 10 search box, type **network**. Then click Change Advanced Sharing Settings on the left side.
2. Click Turn On/Turn Off Network Discovery, and then click the Save Changes button.

Standalone Server   A *standalone server* is not a member of a domain. Many organizations may use this type of server for virtualization. For example, say you load Windows Server 2012 R2 with Hyper-V (Microsoft's virtualization server) on a standalone server. You can then create virtual machines that act as domain controllers to run the network.

Client Machine   A *client machine* is a computer that normally is used by a company's end users. The most common operating systems for a client machine are Windows XP, Windows Vista, Windows 7, Windows 8, and Windows 10.

DNS Server   A *Domain Name Service (DNS)* server has the DNS service running on it. DNS is a name-resolution service that resolves a hostname to a TCP/IP address (called forward lookup). DNS also has the ability to resolve a TCP/IP address to a name (called reverse lookup). When you install an operating system onto a computer, you assign that computer a hostname. The problem is that computers talk to each other by using TCP/IP addresses, for example, 192.168.1.100. It would be very difficult for most users to remember all the different TCP/IP addresses on a network. So normally you connect to a machine by using its hostname. DNS does the conversion of hostname to TCP/IP address for you.

The easiest way to understand how this works is to think of your phone number. If someone wants to call you but doesn't have your telephone number, they can call Information. They give Information your name, and they get your phone number. This is basically how a network works as well. DNS is Information on your network. You give DNS a hostname, and it returns a network telephone number (TCP/IP address). DNS is a requirement if you want to install Active Directory. You can install DNS before or during the Active Directory installation. DNS can help resolve either IPv4 or IPv6 TCP/IP addresses, both of which are explained later in this chapter, in the section "Understanding TCP/IP."

The reason that DNS can resolve both IPv4 and IPv6 is because of the Link Local Multicast Name Resolution, or LLMNR, protocol, which is based on DNS packet formats that allow both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local network.

DHCP Server   A *Dynamic Host Configuration Protocol (DHCP)* server runs the DHCP service, which assigns TCP/IP information to your computers dynamically. Every computer needs three settings to operate properly (with the Internet and intranet): a TCP/IP address, a subnet mask, and a default gateway (router address). Your computers can get this minimum information two ways: manually, where someone manually types in the TCP/IP information on the machine, or dynamically, where the DHCP service automatically assigns the machine an address. DHCP can assign more than just these three settings. DHCP can assign any TCP/IP configuration information, including the address of a DNS server, WINS server, time servers, and so forth.

Continuing with our scenario from "DNS Server," DHCP would be the phone company. DHCP is the component that assigns the telephone number (TCP/IP number).

If you are using DHCP and your Windows 10 machine receives a 169.254.*x.x* TCP/IPv4 address, your client is not able to connect to the DHCP server. Windows 10 machines will automatically assign themselves a 169.254.*x.x* TCP/IPv4 number when DHCP is unavailable. This is called Automatic Private IP Addressing (APIPA). DHCP can issue either IPv4 or IPv6 TCP/IP addresses.

Global Catalog   The *Global Catalog* is a database of all Active Directory objects in a forest with only a subset of the object attributes. Think of the Global Catalog as an index. If you needed to look something up in this Windows 10 book, you would go to the index and find what page you need to turn to. You would not just randomly look through the book for the information. This is the same purpose the Global Catalog serves in your Active Directory forest. When you need to find a resource in the domain (user, published printer, and so forth), you can search the Global Catalog to find its location.

Domain controllers need to use a Global Catalog to help with user authentication. Global Catalogs are a requirement on an Active Directory domain. All domain controllers can be Global Catalogs, but this is not always a good practice. Your network should have at least two Global Catalogs for redundancy, but too many can cause too much Global Catalog replication traffic unless you have a single-domain model.

Location Aware Printing   Location Aware Printing allows you to choose different default printers for different networks. This was introduced in Windows 7, and it allowed your system to connect to the printer that was on your current network. So if you were on your home network, it would automatically print to your home printer, and if you were at work, it work automatically choose your work printer.

One of the objectives listed at the beginning of the chapter was location-aware printing. At the time this book was written, Microsoft announced that the location-aware printing feature that was introduced in Windows 7 was being removed. I listed it in the event that Microsoft adds it back into Windows 10.

Configuring Windows 10 NIC Devices

Before you can connect a Windows 10 machine to the domain, you must set up the *network interface card (NIC)*—a hardware component used to connect computers or other devices to the network to allow the machines to communicate with each other. NICs are responsible for providing the physical connection that recognizes the physical address of the device where they are installed.

> **NOTE**   The Open System Interconnection (OSI) model defines the encapsulation technique that builds the basic data structure for data transport across an internetwork. The OSI model provides interoperability among hardware vendors, network protocols, and applications. The physical address is the OSI model Layer 2 address or, for Ethernet technologies, the MAC (Media Access Control) address. This is not an IP address, which is the OSI Layer 3 or Network Layer address, also generically defined as the logical address.

We generically call the interface between our network devices and the software components of the machines *network adapters* (also referred to as a NIC). Most commonly, you see network adapters installed on computers, but you also see network adapters installed in network printers and specialized devices such as Intrusion Detection Systems (IDSs) and firewalls. Network adapters do not need to be separate cards; they can be built in, as in the case of most PCs today or other network-ready devices such as network cameras or network media players. These adapters (and all other hardware devices) need a driver to communicate with the Windows 10 operating system.

Before you physically install a network adapter, it's important to read the vendor's instructions that come with the hardware. Most network adapters you get today should be self-configuring, using Plug and Play capabilities. After you install a network adapter that supports Plug and Play, it should work following the installation procedure (which should be automated if the vendor says it is). You might have to restart, but our operating systems are getting much better with this, and you might just get lucky and be ready to use the device immediately.

If you happen to have a network adapter that is not Plug and Play, the operating system should detect the new piece of hardware and start a wizard that leads you through the process of loading the adapter's driver and setting initial configuration parameters. You can see your network connection and manage the network connection properties through the Network and Sharing Center.

Configuring a Network Adapter

After you have installed the network adapter, you configure it through its Properties dialog box. You can get to the network adapter properties pages via the Network and Sharing

Center (detailed in the "Configuring Wireless Network Settings" section later in this chapter), through Computer Management, or through Device Manager.

   To use the Device Manager applet for the network adapter configuration, right-click the Start and choose Device Manager. This launches Device Manager (see Figure 9.3) MMC (Microsoft Management Console).

F I G U R E 9 . 3   Device Manager MMC
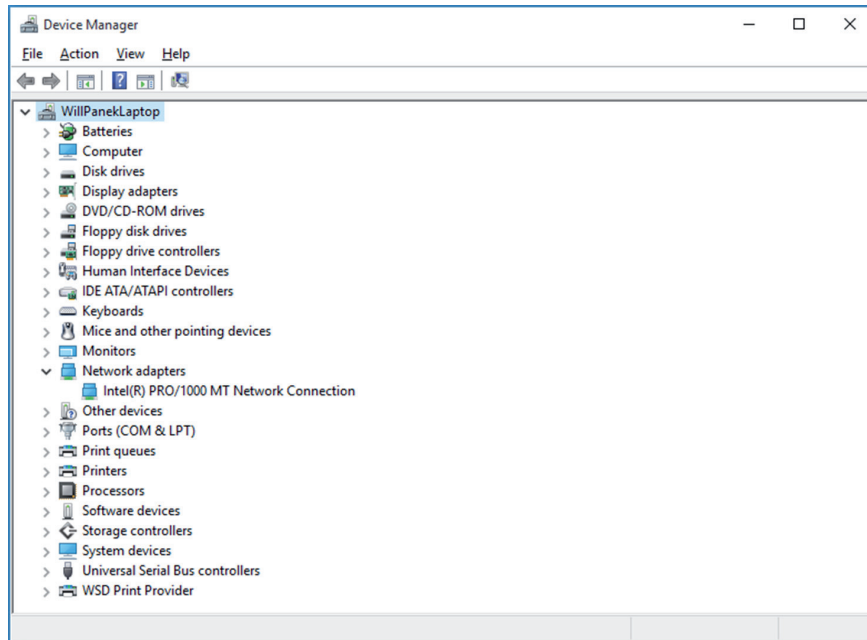
Figure 9.3 shows the Network Adapters device category expanded, and the adapter is installed in the machine. Accessing the network adapter properties allows us to view and change configuration parameters of the adapter. You do this by right-clicking the adapter in Device Manager and selecting Properties from the context menu. Each tab is detailed in the following paragraphs.

General Tab   The General tab of the Network Adapter Properties dialog box (Figure 9.4) 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. If not, the Device Status box gives you an error code and a brief description of what Windows 10 identifies as the issue. You can perform an Internet search for the error code(s) if the text is not sufficient.

FIGURE 9.4   General tab of the Network Adapters Properties page
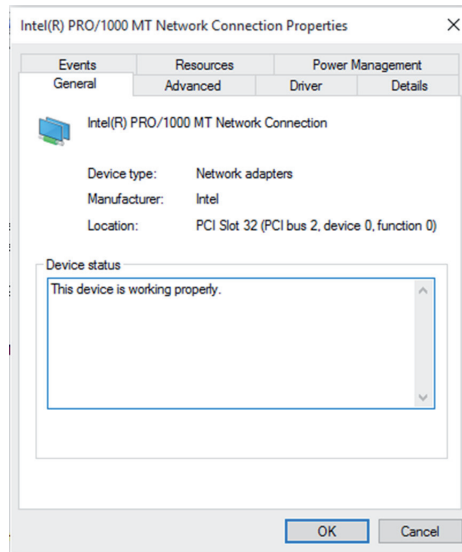
Advanced Tab   The contents of the Advanced tab of a Network Adapter's Properties dialog box vary depending on the network adapter and driver that you are using. Figure 9.5 shows an example of the Advanced tab for my Fast Ethernet adapter. To configure options in this dialog box, choose the property you want to modify in the Property list box and specify the desired value for the property in the Value box on the right. I have selected the Connection Type property and opened the drop-down list box to show you the options for my network adapter.

FIGURE 9.5   Advanced tab of the Network Adapters Properties page
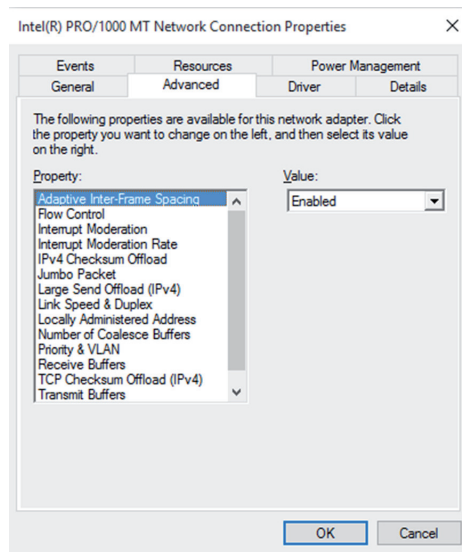
Driver Tab   The Driver tab of the Network Adapters Properties dialog box provides the following information about your driver:

- The driver provider

- The date the driver was released

- The driver version (useful in determining whether you have the latest driver installed)

- The digital signer (the company that provides the digital signature for driver signing)

The Driver tab for my adapter is shown in Figure 9.6. The information here varies from driver to driver and even from vendor to vendor.

FIGURE 9.6   Driver tab of the Network Adapters Properties page
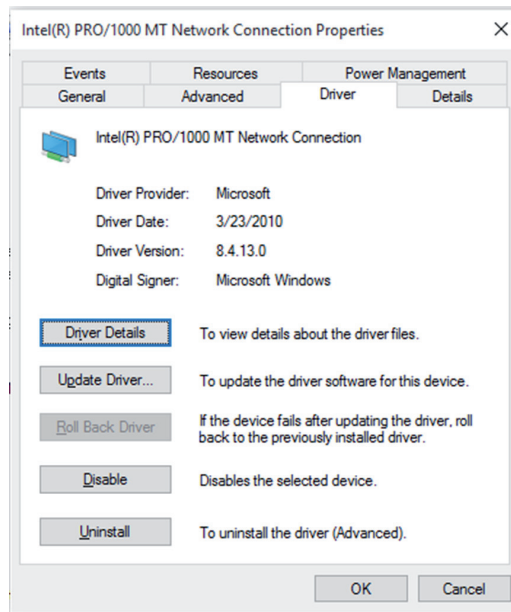
> **The Driver Details button** on the Driver tab brings up the Driver File Details dialog box that provides the following details about the driver:

- The location of the driver file (useful for troubleshooting)

- The original provider of the driver

- The file version (useful for troubleshooting)

- Copyright information about the driver

- The digital signer for the driver

> **The Update Driver button** starts a wizard to step you through upgrading the driver for an existing device.

The Roll Back Driver button allows you to roll back to the previously installed driver if you update your network driver and encounter problems. In Figure 9.6, the Roll Back Driver button is grayed out (not available) because I have not updated the driver or a previous driver is not available.

The Disable button is used to disable the device. After you disable the device, the Disable button changes into an Enable button, which you can use to enable the device.

The Uninstall button removes the driver from your computer's configuration. 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 configuration from your system so you can reinstall it from scratch either automatically or manually.

Details Tab   The Details tab of the network adapter's Properties dialog box lists the resource settings for your network adapter. Information found on the Details tab varies by hardware device. I have included the Details tab information from my adapter in Figure 9.7, with the Property drop-down list box expanded to show the options for my hardware.

FIGURE 9.7   Details tab of the Network Adapter Properties page
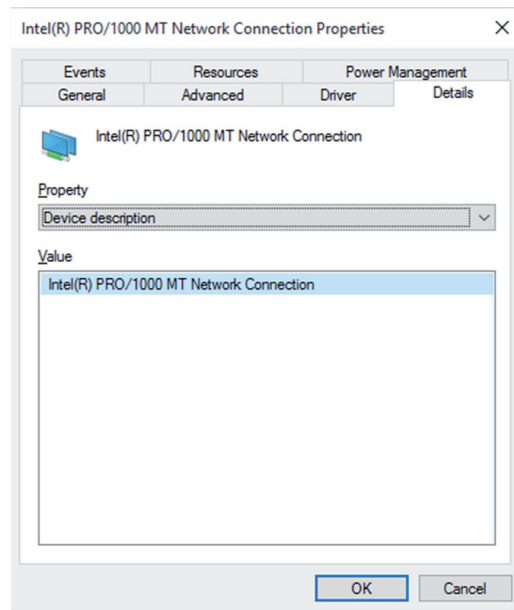
Events Tab   The Events tab (Figure 9.8) of the network adapter's Properties dialog box shows you some of the device events that have happened to this piece of hardware. There is also a View All Events button that opens the Event Viewer MMC, which shows you all events for this device. This is a good way to look to see if there have been any events or issues (like errors or warnings) to the device.

FIGURE 9.8   Events tab of the Network Adapter Properties page
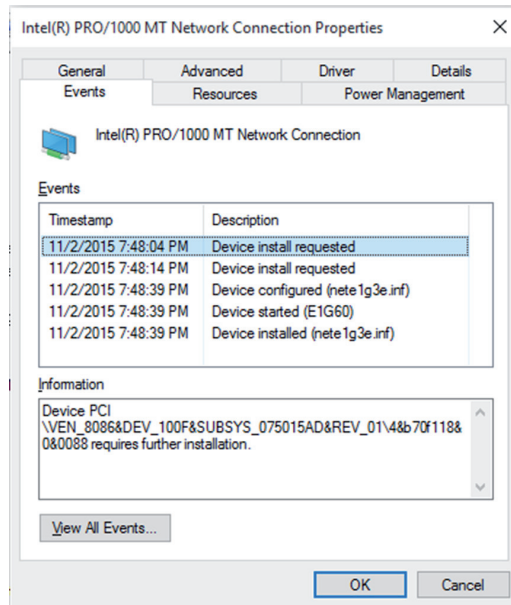
Resources Tab   The Resources tab of the Network Adapter's Properties dialog box (Figure 9.9) lists the resource settings for your network adapter. Resources include interrupt request (IRQ), memory, and input/output (I/O) resources. This information can be important for troubleshooting if other devices are trying to use the same resource settings. This is not normally the case because Windows 10 and the Plug and Play specification should set up nonconflicting parameters. If there are issues, the Conflicting Device List box at the bottom of the Resources tab will show the conflicts.

Power Management Tab   The Power Management tab (Figure 9.10) of the network adapter's Properties dialog box allows you to set up how this device can save power on the system. For example, you can allow the system to turn off this device and also allow this device to wake the system from sleep mode.

FIGURE 9.9 Resources tab of the Network Adapter Properties page
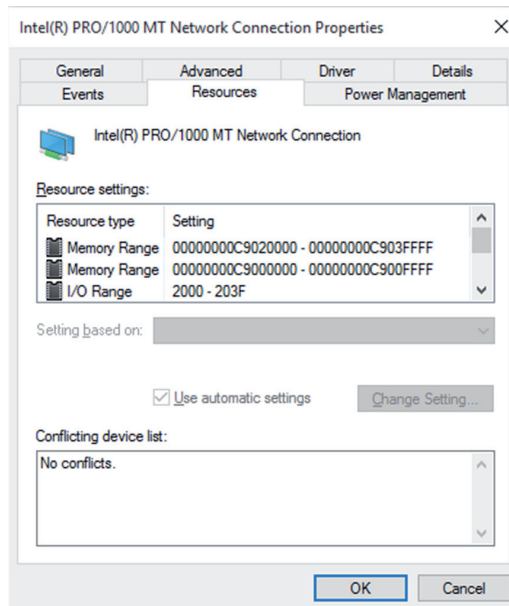
FIGURE 9.10 Power Management tab of the Network Adapter Properties page
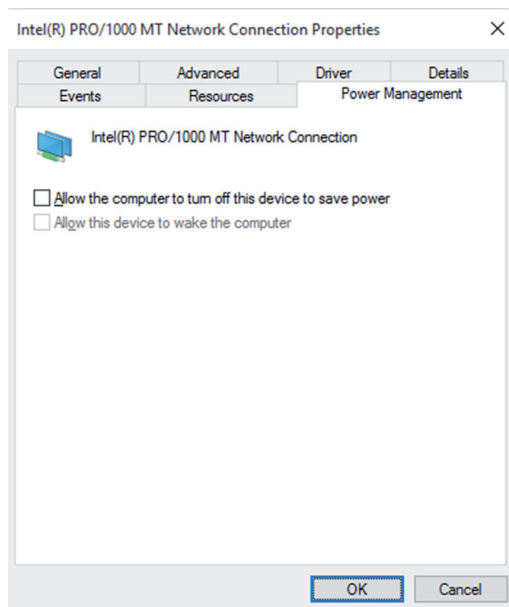
Troubleshooting a Network Adapter

When installing the NIC, you may encounter some problems or errors. Let's take a look at some NIC troubleshooting.

If your network adapter is not working, the problem might be with the hardware, the driver software, or the network protocols. We discuss the Layer 3 (Network Layer) issues later in this chapter in the section "Understanding TCP/IP." The following are some common Layer 1 (Physical Layer) and Layer 2 (Data Link Layer) causes for network adapter problems:

Network Adapter Not on the HCL   If the device is not on the Hardware Compatibility List (HCL), use your Internet resources to see if others have discovered a solution, or contact the hardware vendor for advice.

Outdated Driver   Make sure that you have the most current driver for your adapter. You can have Windows 10 check for an updated driver from the Driver tab of the Properties page for the adapter by clicking the Update Driver button and having Windows search for a better driver, or you can check for the latest driver on the hardware vendor's website.

Network Adapter Not Recognized by Windows 10   Check Device Manager to see whether Windows 10 recognizes the adapter. If you don't see your adapter, you can try to manually install it.

Improperly Configured Network Card   Verify that the settings for the network card are correct for the parameters known within your network and for the hardware device the machine is connected to.

Cabling Problem   Make sure that all network cables are functioning and are the correct type. This includes making sure that the connector is properly seated, the cable is straight or crossed (depending on where it's plugged in), and the cable is not broken. This is usually done by looking at the little green light (LGL) on the network adapter card. This does not guarantee a good connection even if the LGLs are illuminated. A single conductor failure in a cable can still have a link light on, but data is not passing.

Bad Network Connection Device   Verify that all network connectivity hardware is properly working. For example, on a Fast Ethernet network, make sure the switch and port being used are functioning properly.

> **NOTE**   There are seven layers to the OSI model. Starting at Layer 7 and working down, they are Application, Presentation, Session, Transport, Network, Data-Link, and Physical. You can remember this by using the phrase "All People Seem To Need Data Processing."

Configuring Wireless NIC Devices

Wireless technology has matured to the point of becoming cost effective and secure. The use of wireless network adapters is increasingly popular, scaling well out of the home and

into the workplace. Windows 10 supports wireless auto configuration, which makes wireless network connections easy to use. Windows 10 will automatically discover the wireless networks available and connect your machine to the preferred wireless network.

One of the advantages to setting up Windows 10 and wireless connections is that once you have connected to a wireless access point, your Windows 10 will remember that and reconnect you to that preferred wireless network when your Windows 10 system is in range.

Configuring Wireless Network Settings

If you have a wireless network adapter compatible with Windows 10, it will be automatically recognized by the operating system. This can be a built-in adapter such as most modern laptops come with, a wireless card you install in the machine, or even a wireless USB adapter. After it is installed, it is shown in Device Manager as well as in the Network and Sharing Center within the View Your Active Networks section.

We used Device Manager in the previous section for the network adapter configuration, so let's use the Network and Sharing Center for the wireless network configuration. Figure 9.11 shows the Network and Sharing Center with one active network, the Wireless Network Connection called Trend.

FIGURE 9.11   Network and Sharing Center
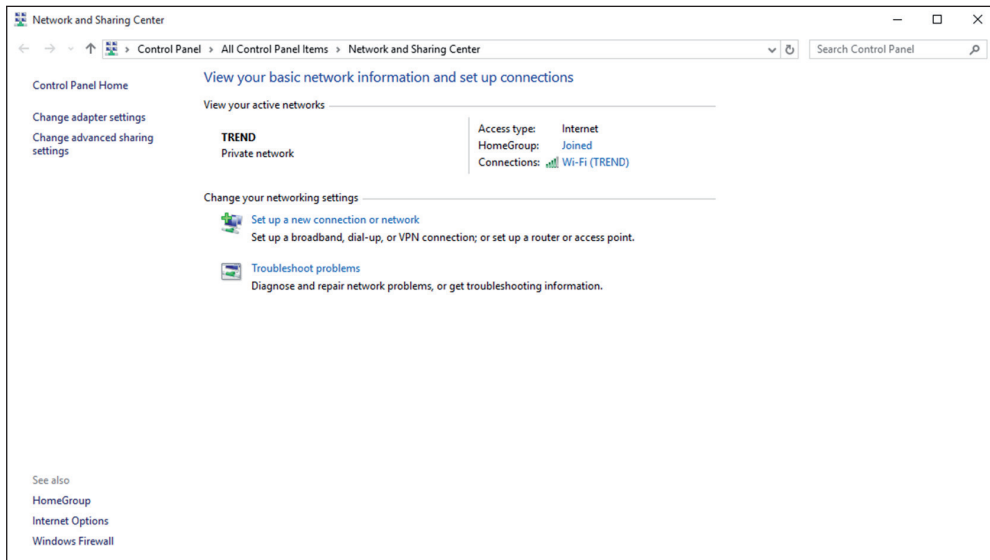
You can perform any of the following steps to access the Network and Sharing Center:

- Type **Network and Sharing Center** in the integrated search box of Windows 10.

- Right-click Start ➢ Control Panel ➢ Network And Internet ➢ Network And Sharing Center (if Control Panel view is Category).

- Right-click Start ➤ Control Panel ➤ Network And Sharing Center (if Control Panel view is Large Icons or Small Icons).

- Right-click the network icon in the lower-right taskbar and choose Open Network And Sharing Center.

- Click Start ➤ Settings ➤ Network and Internet and then choose either the Wi-Fi or Ethernet Connection link.

Viewing the Wireless Network Connection Status

From the Network and Sharing Center, you have easy access to the Wireless Network Connection Status window, which gives you an initial look at the status by providing the Layer 3 connectivity status (IPv4 and IPv6), media state, service set identifier (SSID) being used, how long the connection has been active (Duration), the negotiated speed of the connection, and the signal quality, as shown in Figure 9.12.

FIGURE 9.12   Wireless Network Connection Status
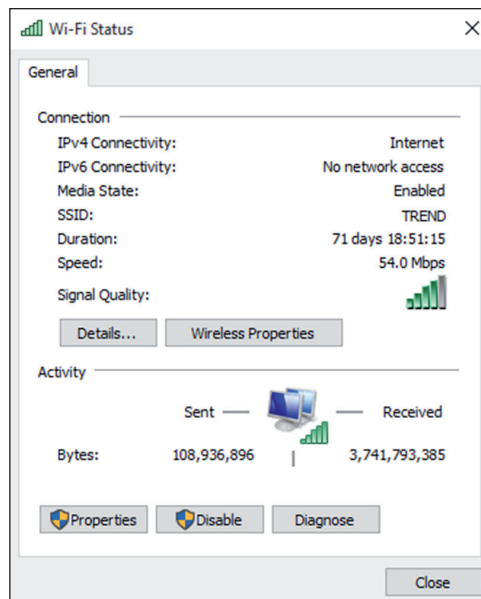
The Details button provides information such as the actual physical address (Layer 2), logical address (Layer 3), dynamic addressing parameters (DHCP), name-resolution items, and more. After verifying Physical Layer parameters, this area is a great place to verify or troubleshoot logical (driver/software) issues.

Viewing Wireless Network Connection Details

If you have a wireless adapter in your machine, perform Exercise 9.1 to view the Network Connection Details for your Wireless Network Connection.

Viewing the Network Connection Details

1. Type **Network and Sharing Center** in the Windows 10 integrated search window; press Enter.

2. Select the Wireless Network Connection menu item from the View Your Active Networks section.

3. Click the Details button.

4. Review the network connection details for this connection.

The Wireless Network Connection Status window has an Activity section showing real-time traffic (in bytes) being sent from and received by the wireless network. From the Wireless Network Connection Status window, you also have access to the Wireless Network Connection Properties, which includes access to the wireless adapter configuration pages.

You access the properties page by clicking the Properties button in the Activity section (refer back to Figure 9.12). The Wi-Fi Properties page has a Networking tab (see Figure 9.13) that shows which network adapter is being used for this connection (which you can change if you have more than one available).

FIGURE 9.13 Wi-Fi Properties window's Networking tab
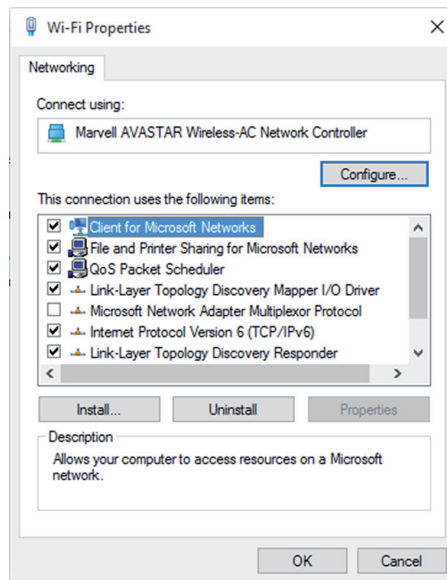
The section that begins with "This connection uses the following items" displays the various clients, services, and protocols that are currently available for this connection.

You can install or uninstall network clients, network services, and network protocols by clicking the appropriate button. You can also view the client, service, or protocol properties if they are available by first highlighting the item from the list and then clicking the Properties button for the selected item. If the Properties button is gray, a properties page is not available for the item. From the Wireless Network Connection Properties window, you even have access to the network adapter's hardware configuration property pages. These are the same pages you have access to from Device Manager.

Perform Exercise 9.2 to access the network adapter properties from the Wireless Network Connection Properties page.

<div style="background:black;color:white;padding:4px;font-weight:bold">EXERCISE 9.2</div>

Viewing Wireless Network Connection Properties

1. Type **Network and Sharing Center** in the Windows 10 integrated search window, and then press Enter.

2. Select the Wireless Network Connection menu item in the View Your Active Networks section.

3. Click the Properties button in the Activity section.

4. Click the Configure button.

5. View the various tabs regarding the network adapter properties.

6. Choose Cancel to return to the Wireless Network Connection Status window.

Configuring Wireless Network Security

Wireless network security is a very large piece of setting up our wireless networks. The focal point for this is the wireless access point or wireless router to which we connect. Whether you are using a small wireless network or a large wireless infrastructure, you should have a plan for secure communication and should configure wireless network security. There are several basic parameters you can configure on your network access devices 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.

- Create a MAC address filter list so only specifically allowed wireless devices can connect to the wireless network, or you can require users attempting to connect to supply connection credentials.

- Enable encryption such as Wi-Fi Protected Access (WPA) or WPA2.

🌐 **Real World Scenario**

Wireless Connection Infrastructure or Ad Hoc?

You might not always be connecting to an access point or router; these connections are considered infrastructure mode connections. An infrastructure mode connection is similar to a wired connection of a PC to an outlet. Instead, you might connect in an ad hoc fashion, which could be a computer-to-computer connection to share information with other wireless network devices without another wireless device acting as an intermediary.

Ad hoc connections exist in a wired environment as well, when we connect two PCs' NICs together by using an Ethernet crossover cable. Securing data transfer in an ad hoc wireless setup is just as important as it is in infrastructure mode, because the data is still traversing between devices using radio frequency (RF), and network sniffers today running the wireless adapter promiscuously (in monitor mode) have no problem viewing the data stream. If the data stream is not encrypted, sniffers will have access to it.

For large implementations, there are several vendors supplying wireless access points under the control of a wireless director, which consists of software-based controllers that are responsible for allowing access points on the network, providing user access control, and enforcing encryption policies. For smaller implementations, this control functionality is done manually as the wireless routers or access points are set up.

The security policies put in place are configured on the wireless access device and the wireless client. Windows 10 client components must be set up to match the security settings of the wireless network access devices. During the setup of most wireless access devices provided by the hardware vendor, the administrator will configure the security parameters. Configuring can be done during the setup program and/or through a web browser that can access the wireless access device configuration pages.

Most of our current devices have a built-in web server to allow the HTTP connection from a web browser. Windows 10 also has the ability to configure the wireless access device if the hardware vendor makes it available. If there is no specific component written, you can launch the web browser–based configuration from a convenient location—the Network and Sharing Center.

Whether you have Windows 10 configure the wireless network connection or you perform the setup through the manufacturer's process, you still need to configure your Windows 10 client access.

If you have performed the simplest configuration and there are no security parameters configured (bad idea, by the way), Windows 10 will connect automatically with a quick window showing the wireless network it's connecting to and providing access without much user intervention. Even canceling the screens will produce a successful (nonsecure) connection. This simple configuration process makes connecting a home or small network easy and straightforward for nontechnical users. However, this is not a good solution.

If you have configured wireless network security (a good idea!), then you need to configure the Windows 10 client with the correct settings. Once again, the configuration screens are available from the convenient location known as the Network and Sharing Center.

In Exercise 9.3, you will access the Windows 10 client wireless network properties.

EXERCISE 9.3

Accessing the Windows 10 Wireless Properties

1. Type **Network and Sharing Center** in the Windows 10 integrated search window; press Enter.

2. Choose the Wireless Network Connection item within the View Your Active Networks section of the Network and Sharing Center.

3. Click the Wireless Properties button (shown in Figure 9.14) within the Connection area of the Wireless Network Connection Status window.

FIGURE 9.14 Wireless Properties button
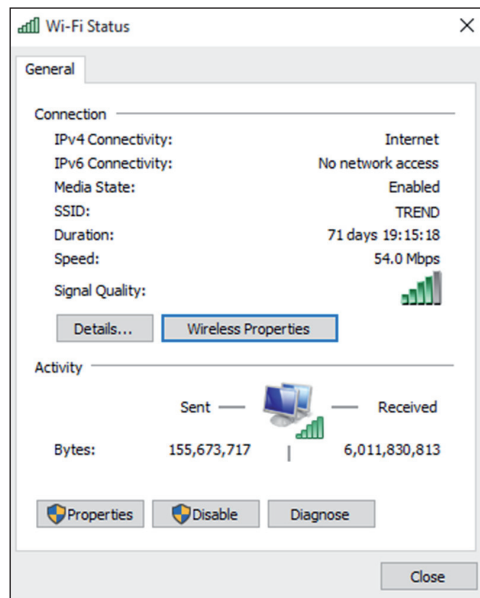
4. The Wireless Network Properties tabbed dialog box opens, displaying the current setup for the wireless network. Click Finish to close the window.

From the Wireless Network Properties tabbed dialog box, you have the ability to set or change the Windows 10 client configuration. The first tab of the dialog box is the Connection tab (Figure 9.15), which displays the following information.

FIGURE 9.15   Wireless Network Properties dialog box's Connection tab
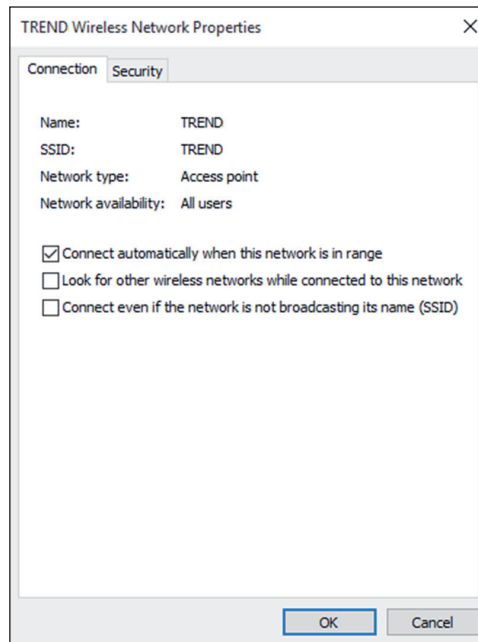
Name   The name assigned to the wireless network.

SSID   The SSID of the wireless connection. This defines a friendly name for the wireless network. This is normally an ASCII string and is usually broadcast by default, allowing a machine or users to select a wireless network with which to connect. Some wireless access devices will allow more than one SSID to be available (broadcast) at the same time, creating more than one wireless network within the same device.

Network Type   Displays the mode the wireless network is operating in. If the wireless network is in infrastructure mode, this parameter will be Access Point. If the wireless network is ad hoc, this will display Computer-To-Computer.

Network Availability   Displays to whom the wireless network is available—All Users or Me Only, for example.

Connect Automatically When This Network Is In Range   This option, when selected, allows automatic connection for this wireless network. Deselecting (clearing the check mark) requires the user to choose this wireless network for connection.

Look For Other Wireless Networks While Connecting To This Network   Windows 10 will attempt to look for other wireless network connections even though you are connected to a network at the time. This allows a user to see if there is a better network connection available even after you have connected to your wireless access point.

Connect Even If The Network Is Not Broadcasting Its Name (SSID)   If the wireless network you are attempting to connect to is not broadcasting its SSID, you must select this option to allow Windows 10 to automatically connect.

The second tab on the Wireless Network Properties dialog box is Security (Figure 9.16), which allows the configuration of the security parameters as defined in your security policy and configured on your wireless network access devices.

Figure 9.16 shows the Security tab's Security Type drop-down box with the WPA-Personal Security choice selected and Encryption Type with TKIP (Temporal Key Integrity Protocol) selected. You can also see the Network Security Key as hidden text because the Show Characters check box is unchecked.

FIGURE 9.16   Wireless Network Properties Security tab
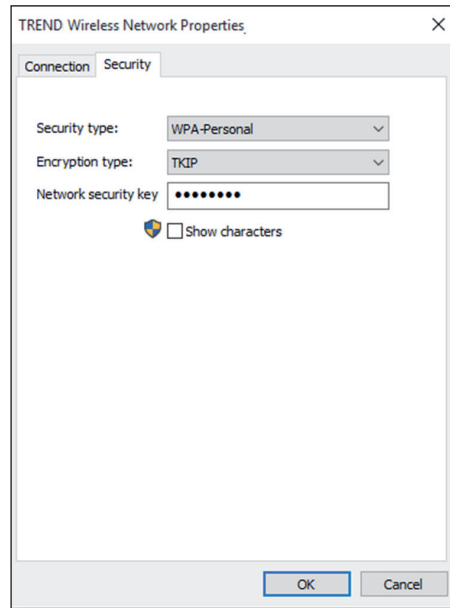
Troubleshooting Wireless Connectivity

There are a few common issues with wireless networking you can look at if you're having problems connecting to your wireless network. Following are a few problems and solutions:

Ensure that your wireless network card is enabled.   Here's one I see regularly: Many newer laptops and tablets have either a switch or a hot-key setting that enables and disables

the wireless device. Often, a laptop switch will somehow be turned off, or a user will somehow press the key sequence to shut off the PC's wireless radio. The Physical Layer is always a good place to start looking.

Ensure that your wireless card and the access devices are compatible.   Cards that are compatible with the 802.11b standard can connect to only 802.11b or 802.11b/g access devices configured to accept b. Cards using 802.11a can connect to only 802.11a or 802.11a/b/g access devices configured to accept a. An 802.11n card needs to connect to an 802.11n access device for efficiency, although most will autonegotiate to the best specification available. The specification you're using on the card has to be available and turned on in the wireless access device.

Ensure that the access point signal is available.   I find radio frequency (RF) to be a funny thing. You can't see it, and you assume that it is everywhere. Not a good assumption. The output power of the signal might be fine, but the RF power is absorbed or attenuated as it goes through walls, insulation, or water. You need to make sure there is nothing that might be causing interference of the wireless signal.

Ensure that the security parameters are configured alike.   The SSID, encryption type, encryption algorithm, and passphrase/security key have to be set the same on both the wireless access device and the wireless client. Here's another one I see quite often: In the desire to make the initial setup and the secure setup easier for end users, some hardware vendors have a nice little button that allows the network access device to negotiate a secure set of parameters with the client. In one instance, after the wireless network had been working correctly for a while, a failure showed the parameters to be incompatible, thanks in large part to someone pressing the easy button just before the failure.

Ensure automatic connections if the SSID is not being broadcast.   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. I have solved several wireless network connection issues with this fix.

Consider how a wireless router interfaces with hard-wired devices.   Many times when I go into a small or midsize network, I find that the company (or home user) is connected to a multifunction type of device. The wireless routers that are often deployed are really quite technologically sophisticated. They have switch ports for connecting hard-wired devices on the private network as well as an Internet port to connect to the outside world. The wireless portion of the device is like another switch port on the private side, allowing the wireless devices to interact with the hard-wired devices.

When I troubleshoot and eliminate issues, I start with the hard-wired devices and see whether they can communicate to each other and the outside (the other side of your wireless router). Try to communicate between the hard-wired and wireless as well, to eliminate the router components. It's also not the best idea to use the wireless network to configure the wireless devices. Configuring through the wireless interface will ultimately cause you to lose connectivity in the middle of a configuration and may force you to connect with the cable, often leaving the access point unusable until you complete the task you started wirelessly.

Understanding TCP/IP

Another item that we need to configure before we can connect a Windows 10 machine to the domain is the protocol that will allow the Windows 10 machine to communicate with other machines. *Transmission Control Protocol/Internet Protocol (TCP/IP)* is the most commonly used network protocol. It is actually a suite of protocols that have evolved into the industry standard for network, internetwork, and Internet connectivity.

> **NOTE**   The main protocols providing 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).

Benefits and Features of TCP/IP

TCP/IP as a protocol suite was accepted as an industry standard in the 1980s and continues to be the primary internetworking protocol today. For a default installation of Windows 10, IPv4 and IPv6 are both 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 at the upper end of the OSI model or the physical components at the lower end of the OSI model.

- TCP/IP provides standard routing services for moving packets over interconnected network segments. Dividing networks into multiple subnetworks (or subnets) optimizes network traffic and facilitates network management.

- TCP/IP is designed to provide data reliability by providing a connection at the Transport layer and verifying that each data segment is received and passed to the application requiring the data by retransmitting lost information.

- TCP/IP allows for the classification of data in regard to its importance with Quality of Service. This allows important time-sensitive streams of data, such as Voice over IP, to get preferential treatment.

- TCP/IP is designed to be fault tolerant. It is able to dynamically reroute packets if network links become unavailable, assuming alternate paths exist.

- Applications can provide services such as Dynamic Host Configuration Protocol (DHCP) for TCP/IP configuration and Domain Name Service (DNS) for hostname-to-IP address resolution.

- Windows 10 continues to support Automatic Private IP Addressing (APIPA) used by small, local-connection-only networks without a DHCP server, to allow Windows 10 to automatically assign an IP address to itself.

- Support for NetBIOS over TCP/IP (NetBT) is included in Windows 10. NetBIOS is a software specification used for identifying computer resources by name as opposed to IP address. We still use TCP/IP as the network protocol, so we map the NetBIOS name to an IP address.

- The inclusion of Alternate IP Configuration allows users to have a static and a DHCP-assigned IP address mapped to a single network adapter. This feature supports mobile users who roam between different network segments.

- IPv6 incorporates a much larger address space compared to IPv4 and, more importantly, incorporates many of the additional features of TCP/IP into a standardized protocol. This is important because a vendor that claims to support TCP/IP only has to support the 1980s version and may not support additional features such as Internet Protocol security (IPSec). IPv6 as a standard includes these features, allowing a more robust network protocol.

Several of the features of TCP/IP included with Windows 10 are as follows:

- Allows a common structure for network communications across a wide variety of hardware and operating systems and a lot of applications that are specifically written to configure and control it.

- TCP/IP connectivity tools allowing access to a variety of hosts across a TCP/IP network. TCP/IP tools in Windows 10 include clients for HTTP, FTP, TFTP, Telnet, Finger, and so forth. Server components for the tools are available to install as well.

- Inclusion of a Simple Network Management Protocol (SNMP) agent that can be used to monitor performance and resource use of a TCP/IP host, server, or network hardware devices.

- TCP/IP management and diagnostic tools for 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, enabling you to print to networked print devices.

- Logical and physical multihoming, enabling 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 enables a Windows 10 computer to route packets among multiple network adapters installed in one machine.

- Support for virtual private networks, which enable you to transmit data securely across a public network via encapsulated and encrypted packets.

Basics of IP Addressing and Configuration

Before you can configure TCP/IP, you should have a basic understanding of TCP/IP configuration and addressing. Let's review TCP/IP addressing. To configure a TCP/IP client, you must specify an IP address, subnet mask, and default gateway (if you're going to communicate outside your local network). Depending on your network, you might want to configure a DNS server, a domain name, or maybe even a WINS server.

You can see the Windows 10 IPv4 Properties window in Figure 9.17. I have included it here because I am going to discuss the different configuration items in the following sections. Although normally set up for automatic configuration, these parameters have been manually assigned in this figure for clarity. Later in this section you will go through the configuration steps and learn how to access this window.

FIGURE 9.17   Windows 10 TCP/IP version 4 properties
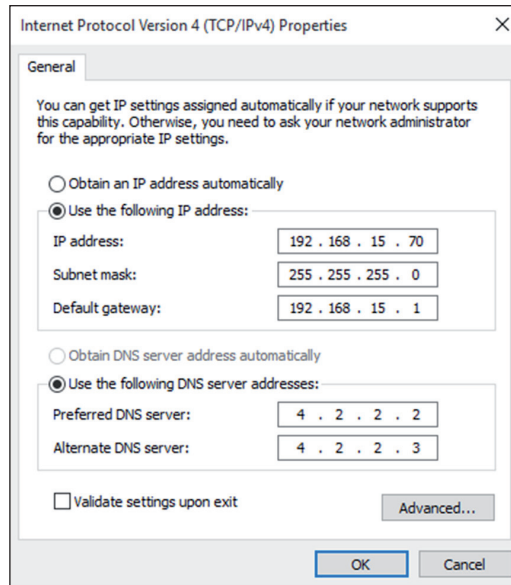
Understanding IPv4 Address Types

The IPv4 address scheme is one of two used by the Internet today, and TCP/IP is the only network protocol used by the Internet. There are three types of IPv4 addresses: broadcast, multicast, and unicast.

A *broadcast address* is read by all hosts that hear it (the broadcast will not go across a router, so only local devices hear the broadcast). The IPv4 broadcast address is 255.255.255.255; every single bit is a 1.

A *multicast address* is a special address that one or more devices will listen for by joining a multicast group. Only the local devices configured to listen for the address will respond and process the data in the multicast packet. A multicast address will have a value between 224 and 239 in the first octet (the leftmost number in the dotted decimal representation). A multicast example is 224.0.0.5.

A *unicast address* uniquely identifies a computer or device on the network. An IPv4 unicast address is a 32-bit address represented as dotted decimal (an example is 131.107.1.200). Each number in the dotted decimal notation is a decimal representation of 8 bits, and the value of each is between 0 and 255 (255 is the numerically largest value that 8 bits can represent). A portion of the IPv4 unicast address is used to identify the network the device is on (or the network of a destination device), and a portion is used to identify the individual host on the local network or the unique host on a remote network.

IPv4 Address Classes

There are three classes of unicast IP addresses defined. Depending on the class you use, different parts of the address show the default network portion of the address and the host address. Table 9.1 shows the three classes of network addresses and the number of networks and hosts available for each network class.

TABLE 9.1 IPv4 class assignments

Network Class	Address Range of First Octet	Number of Unique Networks Available	Number of Unique Hosts per Network
A	1–126	126	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254

> **NOTE** As you probably noticed, 127 is missing from the address ranges. 127.0.0.1 is the diagnostic loopback address, and because of that, no commercial TCP/IP range can start with 127.

The number of octets you can use for either the network ID or the host ID depends on which class you use for your network. For example, if I own a Class B address of 131.107.0.0, the first two octets (131.107) would be the network ID and the last two octets would be the host ID. Table 9.2 shows you the different classes and which octets are the network ID (represented by X) and which octets are the host ID (represented by Y). You are allowed to manipulate only the host IDs (Y) for your organization unless you are using a private IP address scheme.

TABLE 9.2   IPv4 network and host octets

Class	Example	Network ID	Host ID
A	17.1.10.10 (X.Y.Y.Y)	17 (X)	1.10.10 (Y.Y.Y)
B	131.107.14.240 (X.X.Y.Y)	131.107 (X.X)	14.240 (Y.Y)
C	192.168.1.10 (X.X.X.Y)	192.168.1 (X.X.X)	10 (Y)

IPv4 Subnet Mask

The *subnet mask* is used to specify which portion of the unicast IPv4 address defines the network value and which portion defines the unique host value. The subnet mask can be shown either as a dotted decimal, as with 255.255.255.0, or as a slash notation (called Classless Inter-Domain Routing, or CIDR), as in /24. The CIDR representation is the number of bits turned on in the subnet mask. For example, 255.255.224.0 is actually 11111111.11111111.11100000.00000000 (1s are on bits and 0s are off), which equals 19 bits turned on, or /19.

The standard for classful network addressing defines subnet masks for each class, as shown in Table 9.3.

TABLE 9.3   IPv4 default class subnet masks

Class	Default Mask	Slash Notation (CIDR)
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

Another task of the subnet mask is to break down the ranges of your network. For example, 255.255.255.224 allows for six subnets. There should be six TCP/IP ranges that go with the six subnets. Table 9.4 shows the ranges for the different subnet masks.

TABLE 9.4   Subnet mask ranges

Subnet Mask Number	Ranges
255	1
254	2

TABLE 9.4   Subnet mask ranges *(continued)*

Subnet Mask Number	Ranges
252	4
248	8
240	16
224	32
192	64
128	128

What does this chart mean to you? Well, let's say that you have a subnet mask of 255.255.255.224. Because 224 allows for six subnets, the six ranges are in increments of 32. Table 9.5 shows a Class C subnet range for 224. Remember, in any range, you can't use the first number of the range (network ID) or the last number of any range (broadcast).

TABLE 9.5   Class C 224 subnet mask ranges

Subnets	Range	Usable
Range 1	32–63	33–62
Range 2	64–95	65–94
Range 3	96–127	97–126
Range 4	128–159	129–158
Range 5	160–191	161–190
Range 6	192–223	193–222

If this were a Class B subnet mask, the ranges would include a second octet that you would work with. Table 9.6 shows a Class B 224 subnet mask.

TABLE 9.6   Class B 224 subnet mask range

Subnets	Range	Usable
Range 1	32.0–63.255	32.1–63.254
Range 2	64.0–95.255	64.1–95.254

Subnets	Range	Usable
Range 3	96.0–127.255	96.1–127.254
Range 4	128.0–159.255	128.1–159.254
Range 5	160.0–191.255	160.1–191.254
Range 6	192.0–223.255	192.1–223.254

If this were a Class A subnet mask, the ranges would include three octets that you would work with. Table 9.7 shows a Class A 224 subnet mask.

TABLE 9.7 Class A 224 subnet mask range

Subnets	Range	Usable
Range 1	32.0.0–63.255.255	32.0.1–63.255.254
Range 2	64.0.0–95.255.255	64.0.1–95.255.254
Range 3	96.0.0–127.255.255	96.0.1–127.255.254
Range 4	128.0.0–159.255.255	128.0.1–159.255.254
Range 5	160.0.0–191.255.255	160.0.1–191.255.254
Range 6	192.0.0–223.255.255	192.0.1–223.255.254

Using IPv6 Addresses

Through most of this section, we have been referencing TCP/IP as the network protocol. However, you should remember that it is really a suite of protocols running in Layer 3 and Layer 4 of the OSI model. Internet Protocol (IP) is the Layer 3 protocol responsible for assigning devices globally unique addresses (that is, unique in a whole company for private addresses and unique across the whole Internet for public addresses).

When the TCP/IP standard was adopted in the 1980s, it was unimaginable that we would ever need more than 4 billion addresses that are possible with IPv4, but with the dramatic growth of computers in the home and workplace today we do. In the 1990s, programmers realized that a new Layer 3 was going to be needed. This was not an easy task, and integration into the existing infrastructure was going to take a long time. An interim solution known as NAT and PAT emerged. NAT/PAT allowed more than one device to use the same IP address on a private network as long as there was one Internet address available. Cool enough, but this is not the real solution. IPv6 is the solution to the IPv4 address depletion.

As time has progressed from the IPv4 standard acceptance in the 1980s, we have needed new and better functionality. However, the way the standards process works around the world is that you can add functionality, but it may or may not be supported in any vendor's TCP/IPv4 network stack. What happened in IPv6 is not only did the address space increase in size, but the additional functionality that may or may not have been included before has become part of the IPv6 standard.

For example, IPv4 is defined as having a variable-length header, which is cumbersome because we need to read an additional piece of data to see how big the header is. Most of the time, the header stays the same, so why not just fix its length and add an extension to the header if we need to carry more information? IPv6 uses a fixed-length IP header with the capability of carrying more information in an extension to the header, known as an *extension header.*

Microsoft has been including IPv6 in its operating systems since NT 4.0; it just has not been enabled by default. Windows 10 (as did Vista and Windows 7/8) natively supports both IPv4 and IPv6. The main differences you will notice between IPv4 and IPv6 are the format and size of the IP address. IPv6 addresses are 128 bits, typically written as eight groups of four hexadecimal characters. IPv4 addresses, as you saw earlier, are 32 bits—four decimal representations of eight bits. Each of the eight groups of characters in an IPv6 address is separated by a colon; for example, 2001:4860:0000:0000:0012:10FF:FECD:00EF.

Leading zeros can be omitted, so we can write our example address as 2001:4860:0:0:12:10FF:FECD:EF. Additionally, a double colon can be used to compress a set of consecutive zeros, so we could write our example address as 2001:4860::12:10FF:FECD:EF. The IPv6 address is 128 bits; when you see a double colon, it's a variable that says to fill enough zeros within the colons to make the address 128 bits. You can have only one set of double colons; two variables in one address won't work.

Will IPv6 take over the global address space soon? Even with IPv4's lack of address space, we are going to continue to use it for many years. The integration of IPv6 into the infrastructure is going to happen as a joint venture with IPv4 and IPv6 running at the same time in the devices and on some networks.

There are many mechanisms for enabling IPv6 communications over an IPv4 network, including the following:

- Dual stack—A computer or device running both the IPv4 and IPv6 protocol stacks at the same time
- ISATAP—Intra-Site Automatic Tunnel Addressing Protocol
- 6to4—An encapsulation technique for putting IPv6 addresses inside IPv4 addresses
- Teredo tunneling—Another encapsulation technique for putting IPv6 traffic inside an IPv4 packet

Some IPv6-to-IPv4 dynamic translation techniques require that a computer's IPv4 address be 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 2001:4850::F8:192.168.122.26.

There are two ways to receive a TCP/IP address (for either IPv4 or IPv6): You can manually assign a TCP/IP address to the Windows 10 machine, or the Windows 10 machine can use DHCP.

There are several elements of the IPv4 protocol that could use some enhancements. Other elements have been added to IPv4 as extras to provide more functionality. IPv6 is designed to incorporate these enhancement/changes directly into the protocol specification.

The new concepts and new implementation of old concepts in IPv6 include the following:

- Larger address space (128-bit vs. 32-bit).

- Autoconfiguration of Internet-accessible addresses with or without DHCP (without DHCP it's called stateless autoconfiguration).

- More efficient IP header (fewer fields and no checksum).

- Fixed-length IP header (IPv4 header is variable length) with extension headers beyond the standard fixed length to provide enhancements.

- Built-in IP mobility and security (although available in IPv4, the IPv6 implementation is much better implementation).

- Built-in transition schemes to allow integration of the IPv4 and IPv6 spaces.

- ARP broadcast messages are replaced with multicast request.

128-bit Address Space   The new 128-bit address space will provide unique addresses for the foreseeable future. We would like to say we will never use up all the addresses, but history may prove us wrong. The number of unique addresses in the IPv6 space is 2^{128} or 3.4×10^{38} addresses. How big is that number? Enough for toasters and refrigerators (and maybe even cars) to all have their own addresses? Why yes, we believe it is.

For a point of reference, the nearest black hole to Earth is 1,600 light years away. If you were to stack 4mm BB pellets from here to the nearest black hole and back, you would need 7.6×1021 BBs. This means you could uniquely address each BB from Earth to the black hole and back and still have quite a few addresses left over.

Or how about this: the IPv6 address space is big enough to provide well over 1 million addresses per square inch of the surface area of the earth (oceans included). No more running out of addresses for the Internet!

Stateful vs. Stateless Autoconfiguration   Autoconfiguration is another added/improved feature of IPv6. When you are choosing to use DHCP in IPv6, you can choose to set your systems up for Stateful or Stateless configuration. Stateful is what we currently do today with IPv4. Stateful means that DHCP is going to give our IPv6 clients all of their TCP/IP data (IP address, default gateway, and all DHCP options).

What if a Windows 10 client could ask the network itself what network it's on and, based on that information, create its own IP address and default gateway. Well, that is what Stateless configuration does. Stateless configuration means that the client's address is based on the router's advertisement messages. What this means is that the client creates their own

IP address and default gateway based on the router's advertisement message and their MAC address. They can still get all of the other DHCP options, but they will not get an IP address and default gateway from DHCP.

Improved IPv6 Header   The IPv6 header is more efficient than the IPv4 header because it is fixed length (with extensions possible) and has only a few fields. The IPv6 header consists of a total of 40 bytes, which is broken down as follows:

> 32 bytes for source and destination IPv6 addresses

> 8 bytes for version field, traffic class field, flow label field, payload length field, next header field, and hop limit field

We don't waste time with a checksum validation anymore, and we don't have to include the length of the IP header since it's fixed in IPv6; the IP header is variable length in IPv4, so the length must be included as a field.

IPv6 Mobility   IPv6 is only a replacement of the OSI layer 3 component; we are going to continue to use the TCP (and UDP) components as they currently exist; however, a TCP issue is addressed by IPv6. TCP is connection oriented, meaning we establish an end-to-end communication path with sequencing and acknowledgments before we ever send any data, and then we have to acknowledge all pieces of data sent. This is done through a combination of an IP address, port number, and port type (socket).

If the source IP address changes, the TCP connection may be disrupted. But then, how often does this happen? More and more often, because more people are walking around with a wireless laptop or a wireless Voice Over IP (VoIP) telephone. IPv6 mobility adds the capability by establishing a TCP connection with a home address, and when changing networks, it continues to communicate with the original endpoint from a care-of address as it changes LANs, which sends all traffic back through the home address. The handing off of network addresses does not disrupt the TCP connection state (the original TCP port number and address stay intact).

Improved Security   IPv6 has security built in. Internet Protocol security (IPsec) is a component we use today to authenticate and encrypt secure tunnels from a source to a destination. This can be from the client to the server or between gateways. IPv4 lets us do this by enhancing IP header functionality (basically adding a second IP header while encrypting everything behind it). In IPv6, we add this as standard functionality by using extension headers. Extension headers are inserted into the packet only if they are needed. Each header has a "next header" field, which identifies the next piece of information. The extension headers currently identified for IPv6 are Hop-By-Hop Options, Routing, Fragment, Destination Options, Authentication, and Encrypted Security Payload. The authentication header and Encapsulating Security Payload header are the IPsec-specific control headers.

IPv4-to-IPv6 Transmission   There are several mechanisms in place in IPv6 to make the IPv4 to IPv6 transition easy:

A simple dual-stack implementation where both IPv4 and IPv6 are installed and used is certainly an option. In most situations (so far) this doesn't work so well, because most of

us aren't connected to an IPv6 network and our Internet connection is not IPv6 even if we're using IPv6 internally. So Microsoft includes other mechanisms that can be used in several different circumstances.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an automatic tunneling mechanism used to connect an IPv6 network to an IPv4 address space that does not use NAT. ISATAP treats the IPv4 space as one big logical link connection space.

6to4 is a mechanism used to transition to IPv4. This method, like ISATAP, treats the IPv4 address space as a Logical Link Layer with each IPv6 space in transition using a 6to4 router to create endpoints using the IPv4 space as a point-to-point connection (kind of like a WAN, eh?). 6to4 implementations still do not work well through a NAT, although a 6to4 implementation using an Application Layer Gateway (ALG) is certainly doable.

Teredo is a mechanism that allows users behind a NAT to access the IPv6 space by tunneling IPv6 packets in UDP.

Pseduointerfaces are used in these mechanisms to create a usable interface for the operating system. Another interesting feature of IPv6 is that addresses are assigned to interfaces (or pseudointerfaces), not simply to the end node. Your Windows Server 2008 will have several unique IPv6 addresses assigned.

New Broadcast Methods   IPv6 has moved away from using broadcasting. The three types of packets used in IPv6 are unicast, multicast, and anycast. IPv6 clients then must use one of these types to get the MAC address of the next Ethernet hop (default gateway). IPv6 makes use of multicasting for this along with new functionality of neighbor discovery. Not only does ARP utilize new functionality, but ICMP (also a Layer 3 protocol) is redone and known as ICMP6. ICMP6 is used for messaging (packet too large, time exceeded, and so on) as it was in IPv4, but it also is used for the messaging of IPv6 mobility. ICMP6 echo request and ICMP6 echo reply are still used for ping.

Additionally, there are several concepts to consider in IPv6 addressing. The format of the address has changed since IPv4 and we must get used to seeing/using it. There are three types of addresses we will use as well as predefined values used within the address space. You need to get used to seeing these addresses and being able to identify their uses.

IPv6 Address Format

For the design of IPv4 addresses, remember that we present addresses as octets or the decimal (base 10) representation of 8 bits. Four octets add up to the 32 bits required. IPv6 expands the address space to 128 bits, and the representation is for the most part shown in *hexadecimal* (a notation used to represent 8 bits using the values 0–9 and A–F). The following is an example of a full IPv6 address: 2001:0DB8:0000:0000:1234:0000:A9FE:133E.

You can tell the implementation of DNS will make life a lot easier for even those of us who like to ping the address in lieu of the name. Fortunately, DNS already has the ability to handle IPv6 address with the use of an AAAA record. (*A* is short for *alias*.) An A record in IPv4's addressing space is 32 bits, so an AAAA record—4 *As*—is 128 bits. The Windows

Server 2012 R2 DNS server handles the AAAA and the reverse pointer (PTR) records for IPv6.

IPv6 Address Shortcuts

Here are some shortcuts you can use for writing an IPv6 address:

- :0: stands for :0000:
- You can leave out preceding 0s in any 16-bit word.

  For example, :DB8: and :0DB8: are equivalent.
- :: is a variable standing for enough zeros to round out the address to 128 bits.

  :: can be used only once in an address.

You can use these shortcuts to represent the example address 2001:0DB8:0000:0000:1234:0000:A9FE:133E as shown here:

- Compress :0000: into :0:

  2001:0DB8:0000:0000:1234:0:A9FE:133E
- Eliminate preceding zeros:

  2001:DB8:0000:0000:1234:0:A9FE:133E
- Use the special variable shortcut for multiple zeros:

  2001:DB8::1234:0:A9FE:133E

You can also use *prefix notation* or slash notation when discussing IPv6 networks. The network of the example address can be represented as 2001:DB8:0000:0000:0000:0000:0000:0000. This can also be expressed as 2001:DB8:: /32. The /32 indicates 32 bits of network, and 2001:DB8: is 32 bits of network.

IPv6 Address Assignment

So do we subnet IPv6? The answer depends on your definition of subnetting. If you are given 32 bits of network from your ISP, you have 96 bits to work with. If you use some of the 96 bits to route within your network infrastructure, then you are subnetting. In this context you do subnet IPv6. However, given the huge number of bits you have available, we can say with confidence that VLSM will no longer need to be implemented. For example, Microsoft has a network space of 2001:4898:: /32. That gives the administrators a space of 96 bits (2^{96} = 79,228,162,514,264,337,593,543,950,336 unique addresses using all 96 bits) to work with.

We can let Windows Server 2012 R2 dynamically or automatically assign its IPv6 address, or we can still assign it manually. With dynamic/automatic assignment, the IPv6 address is assigned either by a DHCPv6 server or by the Windows Server 2012 R2 machine itself. If no DHCPv6 server is configured, the Windows Server 2012 R2 can query the local LAN segment to find a router with a configured IPv6 interface. If so, the server will assign itself an address on the same IPv6 network as the router interface and set its default gateway to the router interface's IPv6 address.

To see your configured IP addresses (IPv4 and IPv6), you can still use the `ipconfig` command. We have configured a static IPv4 and IPv6 address on our server. The IPv6 address is the same as used in the previous example IPv6 address.

IPv6 Address Types

There are three types of addresses in IPv6: anycast, unicast, and multicast.

> **NOTE** You will notice that there is an absence of the broadcast type that is included in IPv4. IPv6 does not use broadcasts; they're replaced with multicasts.

Anycast Addresses Anycast addresses are not really new. The concept of anycast existed in IPv4 but was not widely used. An anycast address is an IPv6 address assigned to multiple devices (usually different devices). When an anycast packet is sent, it is delivered to one of the devices, usually the closest one.

Unicast Addresses A unicast packet uniquely identifies an interface of an IPv6 device. The interface can be a virtual or *pseudointerface* or a real (physical) interface.

Real World Scenario

Unicast vs. Anycast

Unicast and anycast addresses look the same and may be indistinguishable from each other; it only depends on how many devices have the same address. If only one device has a globally unique IPv6 address, it's a unicast address; if more than one device has the same address, it's an anycast address. Both unicast and anycast are considered one-to-one communication, although you could say anycast is one-to-"one of many."

There are several types of unicast addresses, as described here:

Global Unicast Address As of this writing, the *global unicast address* space is defined as 2000:: /3. 2001::/32 are the IPv6 addresses being issued to business entities. I mentioned before Microsoft has been allocated 2001:4898:: /32. You'll find most example addresses listed as 2001:DB8:: /32; this space has been reserved for documentation. A DHCPv6 server would be set up with scopes (ranges of addresses to be assigned) within this address space. There are some special addresses and address formats you will see in use as well. Do you remember the loopback address in IPv4—127.0.0.1? In IPv6 the loopback address is ::1 (or 0:0:0:0:0:0:0:0001). You may also see an address with dotted decimal used. A dual-stack Windows Server 2012 R2 may also show you FE80::5EFE:192.168.1.200. This address form is used in an integration/migration model of IPv6 (or if you just can't leave the dotted-decimal era).

Link-Local Address *Link-local addresses* are defined as FE80:: /10. If you look at the `ipconfig` command, you will see the link-local IPv6 address as FE80::a425:ab9d:7da4:ccba. The last 8 bytes (64 bits) are random to ensure a high probability of randomness for the link-local address.

The link-local address is to be used on a single link (network segment) and should never be routed.

There is another form of the link-local IPv6 address called the Extended User Interface 64-bit (EUI-64) format. This is derived by using the MAC address of the physical interface and inserting an FFFE between the third and fourth bytes of the MAC. The first byte is also made 02, which sets the universal/local or U/L bit to 1 as defined in IEEE 802 frame specification. Again, looking at `ipconfig`, the EUI-64 address would take the physical (MAC) address 00-03-FF-11-02-CD and make the link-local IPv6 address FE80::0203:FFFF:FE11:02CD. I've left the preceding zeros in the link-local IPv6 address to make it easier for you to pick out the MAC address with the FFFE inserted.

AnonymousAddress Microsoft Server 2012 R2 uses the random address by default instead of EUI-64. The random value is called the AnonymousAddress in Microsoft Server 2012 R2. It can be modified to allow the use of EUI-64.

Unique Local Address The unique local address can be FC00 or FD00 and is used like the private address space of IPv4. Unique local addresses as describe in RFC 4193. They are not expected to be routable on the global Internet. They are routable inside a more limited area, such as a site. They may also be routed between a limited set of sites.

Multicast Address Multicast addresses are one-to-many communication packets. Multicast packets are identifiable by their first byte (most significant byte, leftmost byte, leftmost 2 nibbles, leftmost 8 bits, etc.). A multicast address is defined as FF00::/8.

In the second byte shown (the 00 of FF00), the second 0 is what's called the scope. Interface local is 01; link-local is 02. FF01:: is an interface local multicast.

There are several well-known (already defined) multicast addresses. For example, if you want to send a packet to all nodes in the local link scope, you send the packet to FF02::1 (also shown as FF02:0:0:0:0:0:0:1). The all-routers multicast address is FF02::2.

We also use multicasting to get the logical link Layer address (MAC address) of a device we are trying to communicate with. Instead of using the ARP mechanism of IPv4, IPv6 uses the ICMPv6 neighbor solicitation (NS) and neighbor advertisement (NA) messages. The NS and NA ICMPv6 messages are all part of the new Neighbor Discovery Protocol (NDP). This new ICMPv6 functionality also includes router solicitation and router advertisements as well as redirect messages (similar to the IPv4 redirect functionality).

Table 9.8 outlines the IPv6 address space known prefixes and some well-known addresses.

TABLE 9.8 IPv6 address space known prefixes and addresses

Address Prefix	Scope of Use
`2000:: /3`	Global unicast space prefix
`FE80:: /10`	Local link address prefix
`FC00:: /7`	Unique local unicast prefix
`FF00:: /8`	Multicast prefix
`2001:DB8:: /32`	Global unicast prefix used for documentation
`::1`	Reserved local loopback address
`2001:0000: /32`	Teredo prefix*
`2002:: /16`	6to4 prefix*

IPv6 Integration/Migration

It's time to get into the mindset of integrating IPv6 into your existing infrastructure with the longer goal of migrating over to IPv6. This is not going to be an "OK, Friday the Internet is changing over" rollout. We are going to bring about the change as a controlled implementation. It could easily be three to five years before a solid migration occurs and probably longer. The migration is just below getting the world migrated to the metric system on the overall timeline. The process of integration/migration is made up of several mechanisms:

- Dual stack—Simply running both IPv4 and IPv6 on the same network, utilizing the IPv4 address space for devices only using IPv4 addresses and utilizing the IPv6 address space for devices using IPv6 addresses.

- Tunneling—Using an encapsulation scheme for transporting one address space inside another.

- Address translation—Using a higher-level application to transparently change one address type (IPv4 or IPv6) to the other so end devices are unaware one address space is talking to another.

IPv6 Dual Stack

The default implementation in Windows 10 is an enabled IPv6 configured along with IPv4; this is dual stack. The implementation can be dual IP Layer or dual TCP/IP stack. Windows 10 uses the dual IP Layer implementation. When an application queries a DNS server to resolve a hostname to an IP address, the DNS server may respond with an IPv4 address or an IPv6 address. If the DNS server responds with both, Windows 10 will prefer the IPv6

addresses. Windows 10 can use both IPv4 and IPv6 addresses as necessary for network communication. When looking at the output of the `ipconfig` command, you will see both address spaces displayed.

IPv6 Tunneling

Windows Server 2012 R2 includes several tunneling mechanisms for tunneling IPv6 through the IPv4 address space. They include the following:

- ISATAP—Intra-Site Automatic Tunnel Addressing Protocol used for unicast IPv6 communication across an IPv4 infrastructure. ISATAP is enabled by default in Windows Server 2008.

- 6to4—Used for unicast IPv6 communication across an IPv4 infrastructure.

- Teredo—Used for unicast IPv6 communication with an IPv4 NAT implementation across an IPv4 infrastructure.

With multiple tunneling protocols available and enabled by default, you might ask what the difference is and why one is used over the others. They all allow us to tunnel IPv6 packets through the IPv4 address space (a really cool thing if you're trying to integrate/migrate).

ISATAP   ISATAP is the automatic tunnel addressing protocol providing IPv6 addresses based on the IPv4 address of the end interface (node). The IPv6 address is automatically configured on the local device, and the dual-stack machine can use either its IPv4 or IPv6 address to communicate on the local network (within the local network infrastructure). ISATAP can use the neighbor discovery mechanism to determine the router ID and network prefix where the device is located, thus making intrasite communication possible even in a routed infrastructure.

The format of an ISATAP address is [64 bits of prefix] [32 bits indicating ISATAP] [32 bits IPv4 Address].

The center 32 bits indicating ISATAP are actually 0000:5EFE (when using private IPv4 addresses). The ISATAP address of our example Windows Server 2012 R2 machine using the link-local IPv6 address is FE80::5EFE:192.168.1.200. Each node participating in the ISATAP infrastructure must support ISATAP. If you're routing through an IPv4 cloud, a border router (a router transitioning from an IPv6 to IPv4 space) must support ISATAP. Windows Server 2012 R2 can be configured as a border router and will forward ISATAP packets. ISATAP is experimental and is defined in RFC 4214.

6to4   6to4 specifies a procedure for IPv6 networks to communicate with each other through an IPv4 space without having the IPv6 nodes having to know what's going on.

The IPv6 nodes do not need to be dual stacked to make this happen. The border router is the device responsible for knowing about the IPv6-to-IPv4 transition. The IPv6 packets are encapsulated at the border router and decapsulated at the other end or on the way back. There is an assigned prefix for the 6to4 implementation, 2002:: /16. 6to4 is defined in RFC 3056.

Teredo   Teredo (named after a genus of shipworm that drills holes in the wood of ships) is a protocol designed to allow IPv6 addresses to be available to hosts through one or more layers of NAT. Teredo uses a process of tunneling packets through the IPv4 space using UDP. The Teredo service encapsulates the IPv6 data within a UDP segment (packet) and uses an IPv4 address to get through the IPv4 cloud. Having a Layer 4 (Transport Layer) available to use as a translation functionality is what gives us the ability to be behind a NAT. Teredo provides host-to-host communication and dynamic addressing for IPv6 nodes (dual stack), allowing the nodes to have access to resources in an IPv6 network and the IPv6 devices to have access to the IPv6 devices that have connectivity only to the IPv4 space (just as home users who have an IPv6-enabled operating system connecting to IPv6 resources and their home ISP have only IPv4 capabilities). Teredo is defined in RFC 4380.

In Windows 10, an IPv4 Teredo server is identified and configured (using the `netsh` command interface). The Teredo server provides connectivity resources (address) to the Teredo client (the node that has access to the IPv4 Internet and needs access to an IPv6 network/ Internet. A Teredo relay is a component used by the IPv6 router to receive traffic destined for Teredo clients and forward the traffic appropriately. The defined prefix for Teredo address is 2001:: /32 (does it look better like this? – 2001:0000:: /32). Teredo does add overhead like all the implementations discussed. It is generally accepted that we should use the simplest model available. However, in the process of integration/migration for most of us behind a NAT, Teredo will be the process to choose.

From Windows 10, use the `ipconfig /all` command to view the default configurations including IPv4 and IPv6. You may notice a notation we didn't discuss: the percent sign at the end of the IPv6 address. The number after the percent sign is the virtual interface identifier used by Windows 10.

Information Commands Useful with IPv6

There are numerous commands you can use to view, verify, and configure the network parameters of Windows Server 2012 R2. You can use the `netsh` command set and the `route` command set, as well as the standard `ping` and `tracert` functions.

Use the `netsh` command interface to examine and configure IPv6 functionality (as well as the provided dialog boxes if you like). The `netsh` command issued from the command interpreter changes into a network shell (netsh) where you can configure and view both IPv4 and IPv6 components.

Don't forget to use the ever-popular `route print` command to see the Windows 10 routing tables (IPv4 and IPv6). The other diagnostic commands are still available for IPv4 as well as IPv6. In previous versions of Microsoft operating systems, `ping` was the IPv4 command and `ping6` was the IPv6 command.

This has changed for Windows 10; `ping` works for both IPv4 and IPv6 to test Layer 3 connectivity to remote devices. The IPv4 `tracert` command was `tracert6` for IPv6. The command is now `tracert` for both IPv4 and IPv6 and will show you every Layer 3 (IP) hop from source to destination (assuming all the administrators from here to there want you to see the hops and are not blocking ICMP and also assuming there are not IP tunnels your packets are traversing, you won't see the router hops in the tunnel either).

Overall, the consortium of people making up development of the Internet and Internet protocols have tried to make all changes to communication infrastructures easy to implement (this is a daunting task with so many vendors and various infrastructures currently in place).

The goal is not to daze and confuse administrators; it's to provide the most flexibility with the greatest functionality. IPv6 is going to provide the needed Layer 3 (Network Layer, Global Addressing Layer, Logical Addressing Layer... call it what you like) functionality for the foreseeable future.

Configuring TCP/IP on Windows 10

Windows 10 can use either IPv4 or IPv6 to communicate with other machines on a network, but the Windows 10 machine must receive the TCP/IP address. There are two ways that a Windows 10 machine can get a TCP/IP address: statically or dynamically.

Assigning Static TCP/IP Numbers

As an administrator, it may be necessary to configure a Windows 10 machine manually (static configuration). To do so, you must know the following:

- Which TCP/IP address the machine will receive
- What the subnet mask is for the segment
- What the default gateway (router's TCP/IP address) is
- What the DNS server TCP/IP addresses are

Complete Exercise 9.4 to configure a Windows 10 machine to use a static TCP/IP address. This example uses TCP/IP addresses for a local network, but you can use your own TCP/IP addresses if you know what they should be.

EXERCISE 9.4

Configuring a Static TCP/IP Address

1. Type **Network and Sharing Center** in the Windows 10 integrated search box.

2. In the Network And Sharing Center window, click the Local Area Connection item in the View Your Active Networks section.

3. Click the Properties button from the Activity section of the Local Area Connection Status box.

4. In the Local Area Connection Properties dialog box, click to highlight (do not deselect the check box) Internet Protocol Version 4 (TCP/IPv4) and click the Properties button. Manual configuration will work with both IPv4 and IPv6.

5. Under the General tab, click the Use The Following IP Address radio button. Type in the following (unless you want or know your own settings):

IP Address: **192.168.1.50**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.1.1**

6.   Click the Use The Following DNS Server Addresses radio button and type in **4.2.2.2** (unless you want to use your own settings) in the TCP/IP Address field.

7.   Click OK.

Configuring a Windows 10 Machine to Use DHCP

Dynamic IP configuration assumes that you have a DHCP server on your network that is reachable by the DHCP clients. 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, a Windows 10 machine is configured as a DHCP client for dynamic IP configuration.

Complete Exercise 9.5 to configure a Windows 10 machine to use a dynamic IP configuration.

EXERCISE 9.5

Using DHCP

1.   Type **Network and Sharing Center** in the Windows 10 integrated search box.

2.   In the Network And Sharing Center window, click the Local Area Connection item in the View Your Active Networks section.

3.   Click the Properties button from the Activity section of the Local Area Connection Status box.

4.   In the Local Area Connection Properties dialog box, click to select (do not deselect the check box) Internet Protocol Version 4 (TCP/IPv4) and click the Properties button. DHCP will work with both IPv4 and IPv6.

5.   Choose the Obtain An IP Address Automatically radio button from the General tab of the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.

6.   Choose the Obtain DNS Server Address Automatically radio button from the General tab of the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.

7.   To use this configuration, click OK to accept the selection and close the dialog box. To exit without saving (if you had a valid static configuration), choose Cancel.

If you are using DHCP and you are not connecting to other machines properly, you can type `ipconfig /all` at a command prompt to see what your TCP/IP address is. If your TCP/IP address starts with 169.254.*x.x*, you are not connecting to the DHCP server. Instead, your Windows 10 machine is using APIPA.

Understanding 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, 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 10 under the following conditions:

- When the client is configured as a DHCP client, but no DHCP server is available to service the DHCP request.

- When 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 and the lease period expired.

APIPA uses a Class B network address space that has been reserved for its use. The address space is the 169.254.0.0 network, where the range of 169.254.0.1–169.254.255.254 is available for the host to assign to itself. APIPA uses the following process:

1. The Windows 10 client attempts to use a DHCP server for its configuration, but no DHCP servers respond.

2. The Windows 10 client selects a random address from the 169.254.0.1–169.254.255.254 range of addresses and will use a subnet mask of 255.255.0.0.

3. The client uses a duplicate address-detection method to verify that the address it selected is not already in use on the network.

4. If the address is already in use, the client repeats steps 1 and 2. If the address is not already in use, the client configures its network interface with the address it randomly selected. Given the number of the address the APIPA client can select from (65,534 addresses), the odds of selecting a duplicate are very slim.

5. The Windows 10 network client continues to search for a DHCP server every five minutes. If a DHCP server replies to the request, the APIPA configuration is dropped, and the client receives new IP configuration settings from the DHCP server.

You can determine whether your network interface has been configured using APIPA by looking at your IP address from the command prompt by using the `ipconfig /all` command.

Testing Your IP Configuration

After you have installed and configured the TCP/IP settings, you can test the IP configuration by using the `ipconfig`, `ping`, and `nbtstat` commands. These commands are also useful

in troubleshooting IP configuration errors. You can also graphically view connection details through the Local Area Connection Status section of the Network and Sharing Center.

Using the ipconfig Command

The `ipconfig` command displays your IP configuration. Table 9.9 lists the command switches that you can use with the `ipconfig` command.

TABLE 9.9   `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

Using Other TCP/IP Commands

You can use numerous commands to view, verify, and configure the network parameters of Windows 10. Specifically, you can use the `netsh` command set and the `route` command set, as well as the standard `ping` and `tracert` functions.

Use the `netsh` command interface to examine and configure IPv6 functionality (as well as the provided dialog boxes if you want). The `netsh` command issued from the command interpreter changes into a network shell (netsh) where you can configure and view both IPv4 and IPv6 components.

Don't forget to use the ever-popular `route print` command to see the Windows 10 routing tables (IPv4 and IPv6). In previous versions of Microsoft operating systems, `ping` was the IPv4 command, and `ping6` was the IPv6 command. This has changed for Windows 10; `ping` works for both IPv4 and IPv6 to test Layer 3 connectivity to remote devices. The IPv4 `tracert` command was `tracert6` for IPv6. As already mentioned, the command is now `tracert` for both IPv4 and IPv6 and will show you every Layer 3 (IP) hop from source to destination (assuming all the administrators from here to there want you to see the hops and are not blocking ICMP and also assuming there are no IP tunnels your packets are traversing, or you won't see the router hops in the tunnel either).

TCP/IP Troubleshooting

If you are having trouble connecting to network resources, consider the following:

- If you can access resources on your local subnet but not on a remote subnet, check the default gateway settings on your computer. Pinging a remote host and receiving a Destination Unreachable message is also related to default gateway misconfiguration.

- 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.

- Use the `ipconfig` utility to ensure that you are not configured with an APIPA address. If you are, 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, check the DNS settings on your computer.

After we have TCP/IP set up on our Windows 10 machine, we can connect the Windows 10 machine to the network. In the next section, we will look at how to do that.

Configuring Windows 10 on a Network

In a corporate environment, the client machines (Windows XP, Windows Vista, Windows 7/8/8.1, and Windows 10) will be connected to the domain environment either from the Windows 10 operating system domain or from Active Directory. Having the Windows 10 machine on the network offers many benefits to administration:

- You can deploy GPOs from one location instead of LGPOs on each machine.

- Users can store their data on a server. This way, the nightly backups capture user information. Most Windows 10 machines will *not* be backed up separately.

- You can manage users and groups from one central location (Active Directory) instead of on each Windows 10 machine.

- You can manage resource security on servers instead of on each Windows 10 machine.

Another type of network on which you may have to set up Windows 10 is a HomeGroup environment. HomeGroups allow you to easily connect two or more PCs running Windows 10 on your home network. Windows 10 searches for your home network, and if one is found,

it connects after you enter the HomeGroup password. If a home network is not found, a networking wizard automatically creates a password for the HomeGroup. This password allows you to connect all of your other computers to the same network, and it can be changed any time after the installation of Windows 10.

Adding Windows 10 to the Domain

It does not matter which way you choose to connect the machine to the domain. I usually connect the Windows 10 machine through the Windows operating system, but either way does the same task.

Having the Windows 10 machine on the domain offers many benefits to administration:

- You can deploy GPOs from one location instead of LGPOs on each machine.

- Users can back up their data to a server. This way, the nightly backups cover user information. Most Windows 10 machines will *not* be backed up separately.

- You can manage users and groups from one central location (Active Directory) instead of on each Windows 10 machine.

- You can manage security to resources on servers instead of resources on each Windows 10 machine.

Complete Exercise 9.6 to connect a Windows 10 machine to a Windows Server 2012 R2 domain via the Windows 10 OS. To complete this exercise, you will need to have a Windows Server 2012 R2 domain that the Window 10 machine can connect to.

EXERCISE 9.6

Connecting a Windows 10 Machine to the Domain

1. On the Windows 10 machine, right-click Start and System.

2. Under the Computer Name, Domain, And Workgroup section, click the Change Settings link.

3. Click the Change button next to the To Rename This Computer Or Change Its Domain Or Workgroup section.

4. In the Member Of section, click the Domain radio button (shown in Figure 9.18) and type in the name of your Windows Server 2012 R2 domain.

5. A Credentials box appears, asking for a username and password. Enter an account with administrative credentials to join the machine to the domain. Click OK.

6. A dialog box stating that you are part of the domain appears. Click OK and reboot the machine.

7. From the Windows 10 machine, log on to the domain with your username and password.

FIGURE 9.18   Computer Name/Domain Changes screen
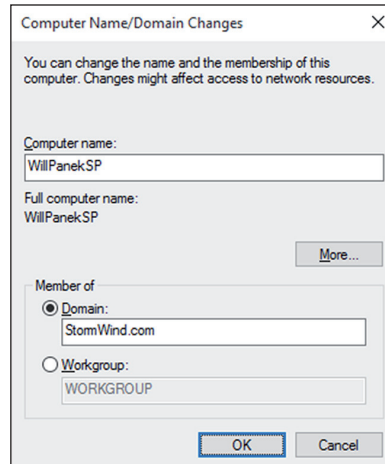
You also have the ability to create the computer account in the Active Directory Users and Computers MMC snap-in. Complete Exercise 9.7 to add the Windows 10 machine to the domain from the Active Directory snap-in. To complete this exercise, you will need a Windows Server 2012 R2 domain that you can add the Windows 10 machine to.

E X E R C I S E 9 . 7

Adding Windows 10 to the Domain via Active Directory

1. From the Windows Server 2012 R2 machine, click Start ➢ Administrative Tools ➢ Active Directory Users And Computers.

2. Expand the domain and right-click the Computers OU. Choose New ➢ Computer.

3. In the Computer Name field, type in the name of the Windows 10 computer. Click OK.

4. Double-click the new Windows 10 computer in the right-hand window to open the properties.

5. Take a look at the different tabs, and then click the Cancel button.

Joining and Sharing HomeGroups in Windows 10

HomeGroup is a function of Windows 10 that simplifies the sharing of music, pictures, and documents within your small office or home network of Windows 10 PCs. HomeGroup allows you to share USB-connected printers too. If you have a printer installed on a Windows 10 computer and it's shared by HomeGroup, it is automatically installed onto the other HomeGroup-enabled Windows 10 PCs. Domain-joined computers cannot host a

HomeGroup, but they can be a participant of a HomeGroup. All editions of Windows 10 can use HomeGroups.

The first step in the process of using HomeGroup for sharing is to create a new HomeGroup or join an existing one. If the Windows 10 network-discovery feature does not find a HomeGroup, you will be asked to create a HomeGroup. In the Control Panel, select the HomeGroup link and then click the Create A HomeGroup button (Figure 9.19).

FIGURE 9.19   Create a HomeGroup.

You will then walk through the Create a HomeGroup wizard. During the wizard, you will be asked what folders you want to share with other members of the HomeGroup (shown in Figure 9.20).

FIGURE 9.20   HomeGroup folders
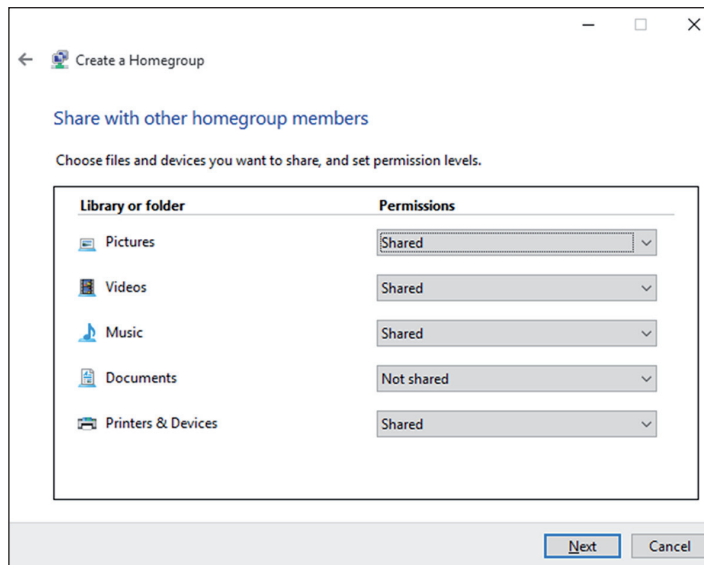
After you have chosen which folders you want to share, you will be given a password that will allow other Windows clients to join the HomeGroup. You can change this password after it has been set by going back into the HomeGroup link (in Control Panel) and choose the Change The Password link.

Now once the HomeGroup is created, other Windows 10 clients can be added. When other Windows 10 clients join the HomeGroup, they will be able to choose the resources that they want to make available to the other members of the HomeGroup. The next step is to enter the HomeGroup password.

Windows 10, by default, will recognize a HomeGroup on the network you're connected to. However, the other Windows 10 machines will not have access to the resources unless they join the HomeGroup. This is very important because allowing just any Windows 10 machine connecting to the network to automatically have shared resource access would be a huge security hole. So to protect Windows 10 user data, a password must be entered to join a HomeGroup before you can access other HomeGroup resources.

After other machines have joined, each machine has the ability to view or change the password. Remember that Windows 10 will initially create a random secure password for the HomeGroup, and you need to visit the View And Print Your HomeGroup Password link to find out what it is. You will probably want to change it. Again, to change the password, choose the Change The Password link from the Change HomeGroup Settings page, as shown in Figure 9.21. When you change the HomeGroup password, you need to go to each of the other Windows 10 machines that are members of the HomeGroup and change the password there if you still want the others to share resources.

FIGURE 9.21   Change HomeGroup Settings screen
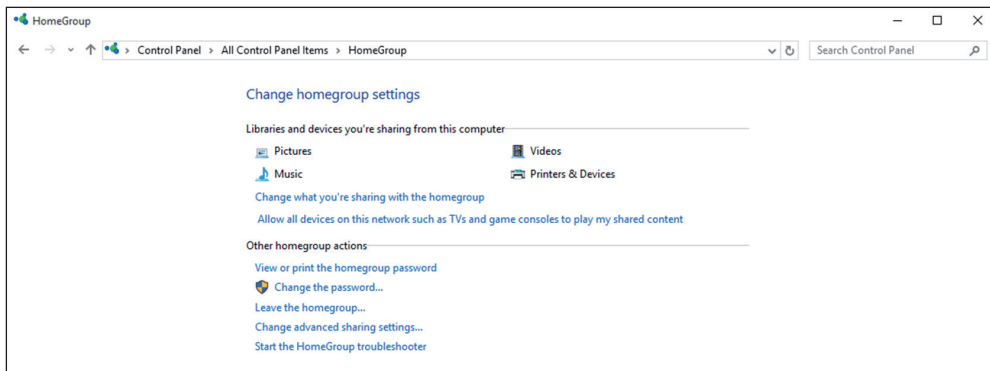
After the HomeGroup is set up, you can see the other members' resources from the HomeGroup option of Windows Explorer or even the Start menu if you customize the Start menu and have added HomeGroup to the displayed options.

HomeGroups are a great option for users who want to share resources in the Windows 10 environment. But what if you still have non–Windows 10 machines? The legacy function of simply sharing resources and setting permissions still works for Windows 10

and will allow older operating systems to have access to resources shared on Windows 10 machines, as well as allow users running Windows 10 to have access to the shared resources on Vista and XP.

Understanding Network Printing

One advantage to setting up any type of network is the ability to use network printers. Network printers are normal printers that are connected to the internal network that users can access.

Think back a few years and remember the days that when you wanted to have a printer, you had to have a print device physically connected to your machine. Now you can just place the print device in a centrally located area, plug it into the network, connect your users to the printer, and start printing.

When it comes to network printing, Windows 10 has made some improvements to help you find and use network printers. One of the improvements is called location-aware printing. Location-aware printing allows a network user to choose different default printers for different networks. For example, you can have a default printer set up at work and a different default printer set up at home. This is very useful for those individuals using laptop computers.

Location-aware printing is available for Windows 10 Professional, Enterprise, and Ultimate editions. Location-aware printing matches the default printer with a network name. This allows you to have different default printers for different networks. Windows 10 can retrieve the network name from multiple sources, such as the name of the domain the Windows 10 machine is connected to or the station identification of the wireless router at your home.

To configure location-aware printing, go into the Devices and Printers Control Panel application. Then select the installed printer and click the Manage Default Printers command in the menu bar on top. Once the Manage Default Printers dialog box opens, you can select a different default printer for each network you visit.

> Location-aware printing was removed in the November 2015 update. But it is still listed as a Microsoft test objective, so we added it to be safe.

Configuring Windows Firewall

Windows Firewall, which is included with Windows 10, helps prevent unauthorized users or malicious software from accessing your computer. Windows Firewall does not allow unsolicited traffic, which is traffic that was not sent in response to a request, to pass through the firewall.

Understanding the Windows Firewall Basics

You configure Windows Firewall by right-clicking Start ➢ Control Panel ➢ Large Icons View ➢ Windows Firewall. You can then decide what firewall options you want to set

(as shown in Figure 9.22) like changing firewall notifications, turning the Windows Firewall on or off, restoring defaults, setting advanced settings, and troubleshooting.

FIGURE 9.22 Windows Firewall settings dialog box
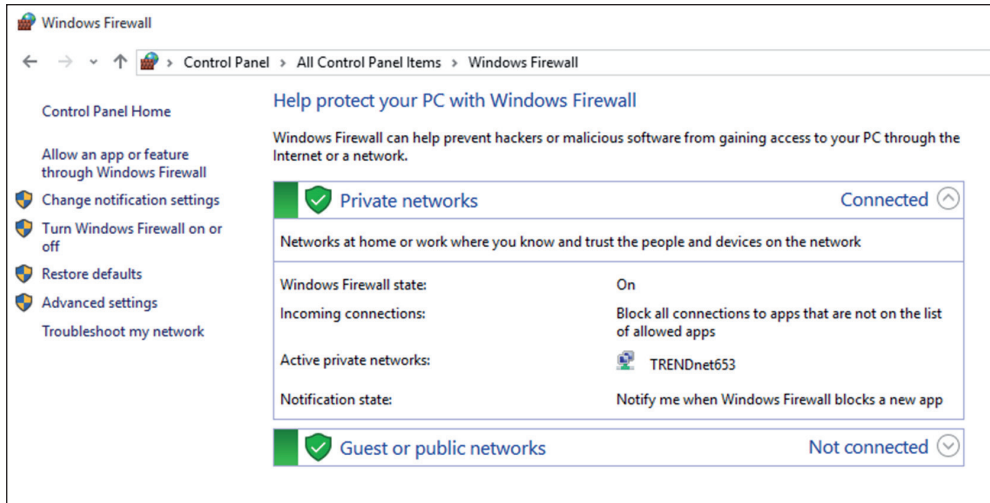
The Windows Firewall settings dialog box allows you to turn Windows Firewall on or off for both private and public networks. The On setting will block incoming sources, and the Turn off Windows Firewall setting will allow incoming sources to connect.

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, all incoming connections (even ones allowed in the allowed apps list) will be blocked by Windows Firewall.

Windows Firewall with Advanced Security

You can configure more-advanced settings by configuring Windows Firewall with Advanced Security (WFAS) by right-clicking Start ▷ Control Panel ▷ Large Icons View ▷ Windows Firewall ▷ Advanced Settings. The Windows Firewall With Advanced Security dialog box appears, as shown in Figure 9.23.

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 when no rule is selected in the left pane. When a rule is selected, the central area shows the rule's settings. The right pane shows the same actions as the Action menu on the top. These are just shortcuts to the different actions that can be performed in Windows Firewall. Let's take a more detailed look at some of the elements in Windows Firewall.

FIGURE 9.23   Windows Firewall With Advanced Security
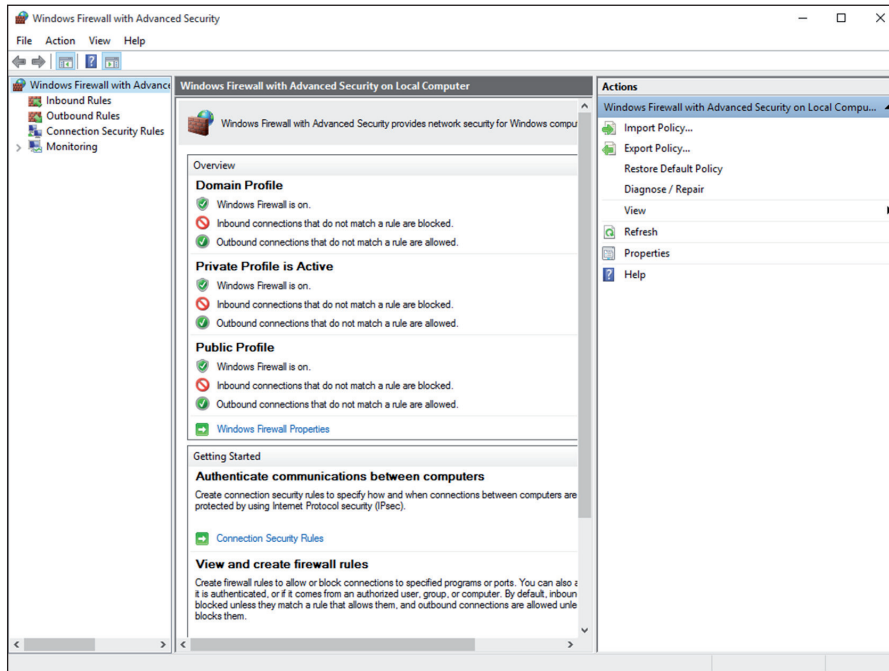
Inbound and Outbound Rules

Inbound and outbound rules consist of many preconfigured rules that can be enabled or disabled. Obviously, inbound rules (see Figure 9.24) monitor inbound traffic, and outbound rules monitor outbound traffic. By default, many are disabled. Double-clicking a rule will bring up its Properties dialog box (Figure 9.25).

You can filter the rules to make them easier to view. Filtering can be based on the profile the rule affects, on whether the rule is enabled or disabled, or on the rule group. You can filter a rule by clicking which filter type you want to use in the right pane or by clicking the Actions menu on the top of the screen.

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 and 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, pre-defined category, or custom settings.

As you are setting up the firewall rules, you have the ability to configure authenticated exceptions. No matter how well your system security is set up, there are almost always times when computers on your network can't use IPsec. This is when you set up authenticated exceptions. It's important to understand that when you set up these authenticated exceptions, you are reducing the security of the network because it allows computers to send unprotected IPsec network traffic. So make sure that the computers that are added to the authenticated exceptions list are managed and trusted computers only.

FIGURE 9.24 Inbound rules
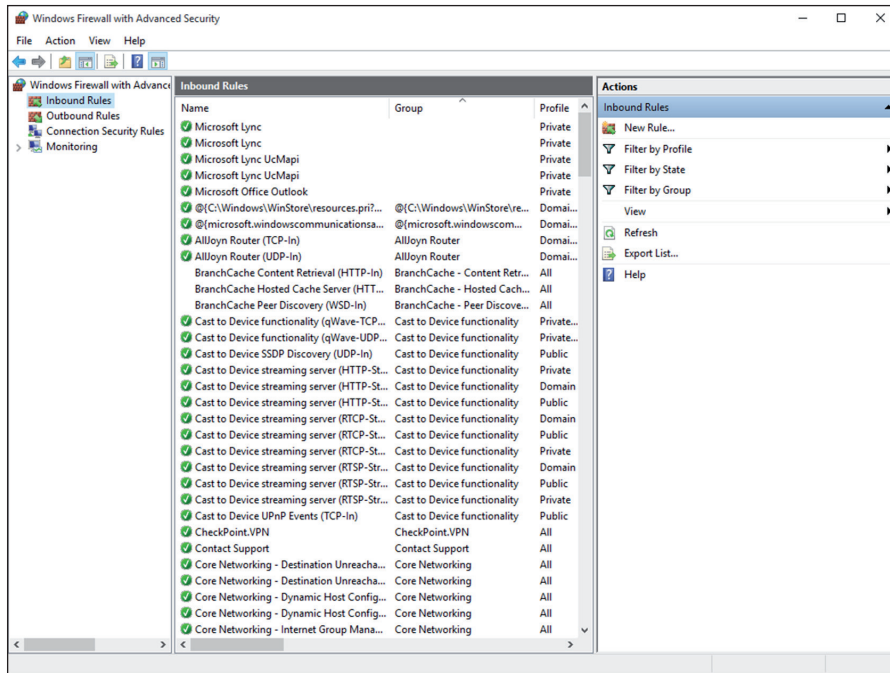
FIGURE 9.25 An inbound rule's Properties dialog box
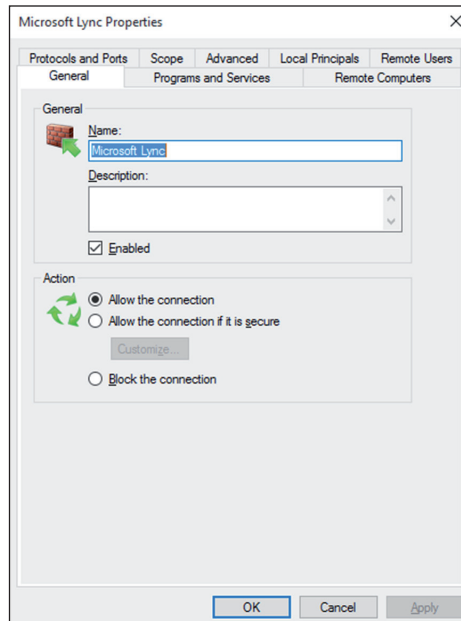
Complete Exercise 9.8 to create a new inbound rule that will allow only encrypted TCP traffic.

EXERCISE 9.8

Creating a New Inbound Rule

1. Right-click Start ➤ Control Panel ➤ Large Icon View ➤ Windows Firewall.

2. Click Advanced Settings on the left side.

3. Right-click Inbound Rules and select New Rule.

4. Choose a rule type. For this exercise, choose Custom so you can see all the options available to you. Then click Next.

5. At the Program Screen, choose All Programs. Then click Next.

6. Choose the protocol type, as well as the local and remote port numbers that are affected by this rule. For this exercise, choose TCP, and ensure that All Ports is selected for both Local Port and Remote Port. Click Next to continue.

7. At the Scope Screen, choose Any IP Address for both local and remote. Then click Next.

8. At the Action screen, choose Allow The Connection Only If It Is Secure. Click Next.

9. At the Users screen, you can experiment with these options if you want by entering users to both sections. Once you click one of the check boxes, the Add and Remove buttons become available. Click Next to continue.

10. At the Computers screen, you can choose what computers you will authorize or allow through this rule (exceptions). Again, you can experiment with these options if you want. Click Next to continue.

11. At the Profiles screen, choose which profiles will be affected by this rule. Select one or more profiles and click Next.

12. Give your profile a name and description, and then click Finish. Your custom rule will appear in the list of inbound rules, and the rule will be enabled.

13. Double-click your newly created rule. Notice that you can change the options that you previously configured.

14. Delete the rule by right-clicking the new rule and choosing Delete. A dialog box will appear asking you if you are sure. Click Yes.

15. Close the Windows Firewall.

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 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.

🌐 **Real World Scenario**

Use More Than Just Windows Firewall

When doing consulting, it always makes me laugh when I see small to midsize companies using Microsoft Windows Firewall and no other protection. Microsoft Windows Firewall should be your last line of defense. You need to make sure that you have good hardware firewalls that separate your network from the world.

Also watch Windows Firewall when it comes to printing. I have run into many situations where a printer that needs to communicate with the operating system has issues when Windows Firewall is enabled. If this happens, make sure that the printer is allowed in the Allowed Programs section.

Summary

In this chapter, we discussed the different types of Windows networks: domain based and peer-to-peer (workgroup) based. We also discussed a newer, easier way to set up a workgroup-based network by using HomeGroups.

Computers need to use a communication device called a NIC device in order to communicate with each other across the network. You can set up Windows 10 to use both wired and wireless NIC devices. Windows 10 also has new features included to help with setting up your wireless networks.

To allow computers to communicate on a network, you must use a *protocol*—a set of communication standards that all computers will use. The main protocol that Windows 10 uses is TCP/IP. There are two versions of TCP/IP that Windows 10 can use, IPv4 and IPv6. IPv4 is the most commonly used protocol, but IPv6 is the newest version of TCP/IP and gives organizations flexibility and growth potential.

Finally, we also discussed using Windows Firewall with Advanced Security. Windows Firewall helps prevent unauthorized users from connecting to the Windows 10 operating system. Windows Firewall is an extra line of defense, but it *should not* replace a perimeter firewall for your network.

Video Resources

There are videos available for the following exercises:

9.1

9.2

9.4

You can access the videos at `www.wiley.com/go/sybextestprep` on the Other Study Tools tab.

Exam Essentials

Understand Microsoft networking.   Know the difference between the Microsoft networks that you can set up. Know the difference between workgroups and domains. Know about working with Azure Active Directory vs. Onsite Active Directory.

Understand how to configure network settings.   Know how to install and configure both wired and wireless networks. Understand how Windows 10 has built-in wireless network support. Know how to set up your preferred wireless network.

Understand IPv4 and IPv6.   Know and understand IPv4 and IPv6. Understand how to configure and maintain both IPv4 and IPv6 networks. Know how to subnet an IPv4 network. Understand that APIPA will automatically assign an IP address to a Windows 10 machine if DHCP is not available.

Know how to configure Windows Firewall.   Know how to set up and maintain Windows Firewall with Advanced Security. Know that you can set up inbound and outbound rules by using Windows Firewall. Know how to allow or deny applications by using Windows Firewall.

Review Questions

1. You are the network administrator for a small organization that has decided to implement Microsoft Active Directory. Your organization is worried because the budget does not allow them to purchase new hardware for the Active Directory installation. The server room has a UNIX server it uses for file and DNS access. What option can you tell them about that will allow the organization to have Active Directory?

    A. Use Microsoft OneDrive to install Active Directory.

    B. Install Active Directory on the UNIX system.

    C. Subscribe to Azure Active Directory.

    D. Tell them that without the new hardware, there is no way to install Active Directory.

2. You are the network administrator for a midsize company that uses Windows Server 2012 R2 and Windows 10. All Windows 10 machines receive their IP address from DHCP. You have a Windows 10 machine and need to identify its IPv6 address. How can you accomplish this task? (Choose all that apply.)

    A. Click Details from the network connection status.

    B. Type `ipconfig /all` at the command prompt.

    C. Type `ipconfig /view` at the command prompt.

    D. Choose Properties of My Computer.

3. You are hired by friends to set up a network in their home. They have four Windows 10 devices in their home that are all connected by a router. There is currently no network in place. They want to be able to share audio and video files among their family members. How can you set up the network? (Choose two.)

    A. Install a Windows Server 2012 R2 domain controller.

    B. Create a HomeGroup.

    C. All audio and video files should be moved to the media library and accessible through HomeGroup.

    D. Move all audio and video files to a shared folder on the Windows Server 2012 R2 machine.

4. You are the network administrator for an organization with two sites, as shown in Figure 9.26. You need to install a new Windows 10 machine into site 1. Which TCP/IP address can you assign to the new Windows 10 machine?

    A. 192.168.2.32

    B. 192.168.2.31

    C. 192.168.2.41

    D. 192.168.2.63

FIGURE 9.26 Network layout
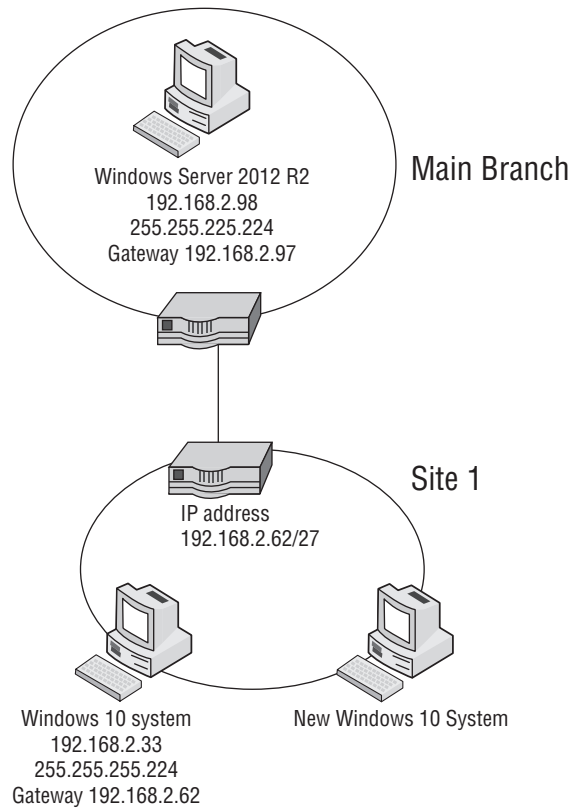
5. You are the network administrator for a large organization that has decided to use IPv6 and DHCP. You want to set up the network so that all Windows 10 systems using IPv6 get all of their information through DHCP including IP address and default gateway. How would you set up the network?

   A. Set up a stateful network.

   B. Set up a stateless network.

   C. Set up DNS to use DHCP.

   D. Set Active Directory static IP addresses.

6. You are the network administrator for a midsize company that uses both desktops and laptops. All laptops use Windows 10 and have been connected to a wireless access point. You disable the SSID, and now your laptops can no longer connect to the access point. What do you need to do to allow the laptops to connect?

   A. Reboot the laptops.

   B. Modify the wireless network connection settings on the laptops.

    C. Reboot the access point.

    D. Disconnect and reconnect the laptops to the domain.

7. You have a Windows 10 system that is having issues connecting to other machines on the network. You want to see the TCP/IP details to make sure that the user is using DHCP and that the assigned IP address is accurate. What command-line utility and switch can you use to do this?

    A. `Route Add`

    B. `Ipconfig /FlushDNS`

    C. `Ipconfig /all`

    D. `Tracert`

8. You are the network administrator for a midsize company that uses both desktops and laptops. All laptops use Windows 10 and have been connected to a wireless access point that is configured to use Advanced Encryption Standard (AES) security. There is no pre-shared password key being used. You need to connect a new Windows 10 laptop to the access point. How would you set up the security setting on the laptop?

    A. WPA2-Personal

    B. WPA2-Enterprise

    C. WPA-Personal

    D. WAP security

9. You are the network administrator for a large organization that uses Windows Server 2012 R2 and Windows 10. You have decided to set up a tunnel between two locations. You want to set the tunnel up so that it uses IPv6. What protocol can you use that allows for IPv4 and IPv6 on your network and to use IPv6 with the tunneling?

    A. IPv4to6

    B. 6v4

    C. ISATAP

    D. TUNISA

10. You are the network administrator for a small organization that has decided to switch the company's TCP/IP subnet mask. The organization has chosen to use 255.255.255.240. What is the increment for subnet ranges in a 240 subnet mask?

    A. 4

    B. 8

    C. 16

    D. 32

Chapter

10

Configuring Recovery

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **Configure system recovery.**

■ This objective may include but is not limited to the following subobjectives: Configure a recovery drive, configure system restore, perform a refresh or recycle, perform a driver rollback, configure restore points.

✓ **Configure file recovery.**

■ This objective may include but is not limited to the following subobjectives: Restore previous versions of files and folders, configure File History, recover files from OneDrive.

Every administrator should take measures to safeguard against disaster. Keeping backups is an important component of disaster preparedness and recovery. Windows 10 has a full backup and restore application (Backup and Restore [Windows 7]) to enable you to maintain a backup copy of any of the Windows 10 component files and data files that are considered critical to the operation of your day-to-day business. You can use the backup of the files to restore files if they become unusable for various reasons such as becoming corrupt, deleted, or even modified.

If you can't start Windows 10, 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 (details on these options are provided throughout the chapter):

- Event Viewer

- Safe Mode

- Last Known Good Configuration

- Startup Repair tool

- Backup and Restore Center

- Driver Rollback

- System Restore

Safeguarding and Recovery Basics

One of the worst events you may 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 ensure to take proactive measures to plan your recovery before the failure occurs. Here are some of the preparations you can take:

- Keep your computer up to date with Windows Update (covered in Chapter 1, "Installing Windows 10").

- 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.

No matter how many safeguards you enact, eventually you'll likely need to recover a system. Table 10.1 summarizes all of the Windows 10 utilities and options you can use to assist in performing system recovery. All these Windows 10 recovery techniques are covered in detail in this chapter.

TABLE 10.1   Windows 10 recovery techniques

Recovery Technique	When to Use
Event Viewer	If the Windows 10 operating system can be loaded through normal mode 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 10. 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.
Startup Repair tool	If your computer will not boot to Safe Mode, you can use the Startup Repair tool to replace corrupted system files. This option will not help if you have hardware errors, however.
Backup and Restore	You should use this utility to safeguard your computer. If necessary, you can use the Backup and Restore (Windows 7) utility to restore personal files from backup media and to restore a complete image of your computer.
Driver Rollback	If you install a driver that causes issues on your system, you can use the Driver Rollback utility to return the driver to its previous version. Use Device Manager to access the Driver Rollback utility. Right-click the hardware component and choose Properties. Then click the Driver tab, and the Roll Back Driver button (Driver Rollback) will be there.
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 version of the checkpoint.

Using Advanced Boot Options

The Windows 10 advanced boot options can be used to troubleshoot errors that keep Windows 10 from successfully booting. Figure 10.1 shows the Advanced Boot Options screen. These advanced boot options are covered in this section.

FIGURE 10.1 Advanced Boot Options screen
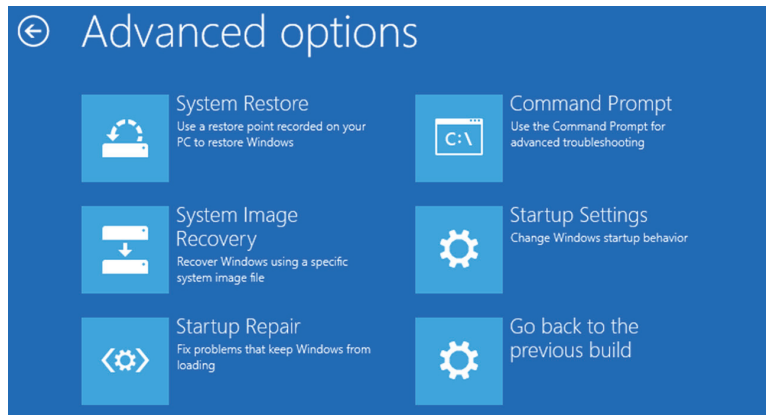
> **NOTE** To access the Windows 10 advanced boot options, start or reboot the computer and press the F8 key after the firmware POST process but before Windows 10 is loaded. This will bring up the Advanced Boot Options menu, which offers numerous options for booting Windows 10.

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 10 will not load, you can attempt to load the operating system in *Safe Mode*. When you run Windows 10 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 ones 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 10 that you have access to when you boot normally, including networking capabilities.

Windows 10 offers a few Startup settings when you're trying to repair your Windows 10 system. Figure 10.2 shows the Startup Settings that are offered when you boot into Startup Settings.

FIGURE 10.2 Startup Settings screen
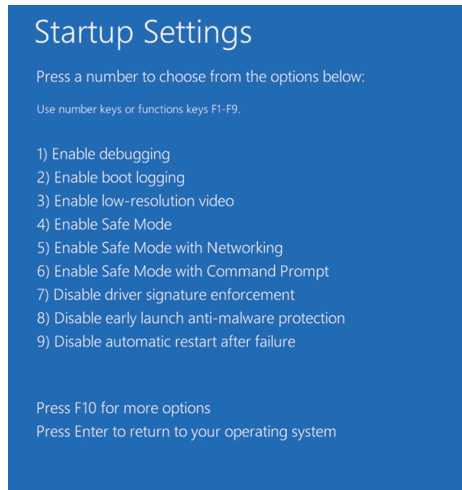
When the Startup Settings screen appears, you then have the ability to choose to enter a Safe Mode (three versions). Once a computer is booted into Safe Mode, you will see the text *Safe Mode* in the four corners of your desktop, as shown in Figure 10.3.

FIGURE 10.3 A computer running in Safe Mode
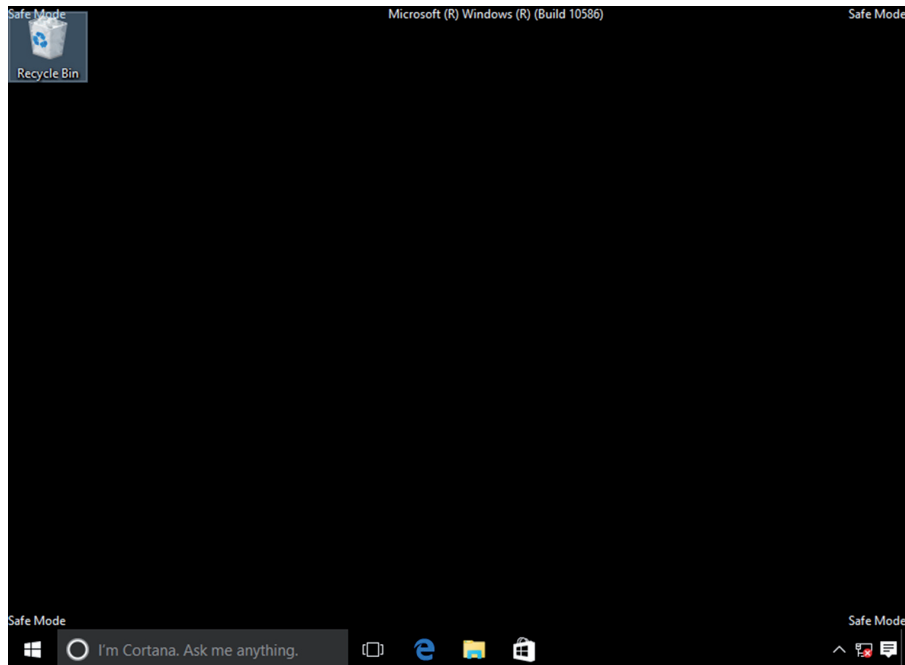
If you boot to Safe Mode, check all of your computer's hardware and software settings in Device Manager and try to determine why Windows 10 will not boot properly. After you take steps to fix the problem, try to boot to Windows 10 as you normally would.

In Exercise 10.1, you will boot your computer to Safe Mode.

EXERCISE 10.1

Booting Your Computer to Safe Mode

1. Turn on the Windows 10 system.

2. During the boot process, press the F8 key to access the Boot Options menu.

3. At the Recovery screen, choose See Advanced Repair Options, as shown in Figure 10.4.

> **FIGURE 10.4** Recovery screen
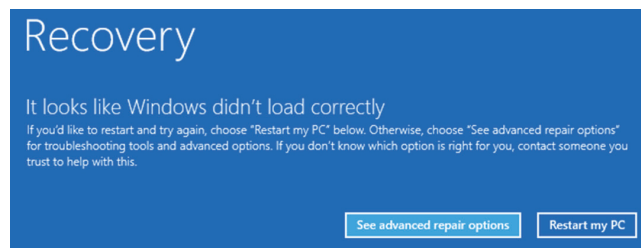
4. At the Choose An Option screen, choose the Troubleshoot option.

5. At the Troubleshoot screen, choose Advanced Options (shown in Figure 10.5).

> **FIGURE 10.5** Troubleshoot screen
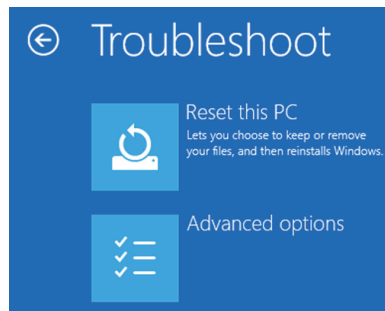
6. At the Advanced Options screen, choose Startup Settings.

7. At the Startup Settings screen, click the Restart button. The system will reboot into the Startup Settings screen.

8. At the Startup Settings screen, choose 5) Enable Safe Mode With Networking.

9. When Windows 10 starts, log in.
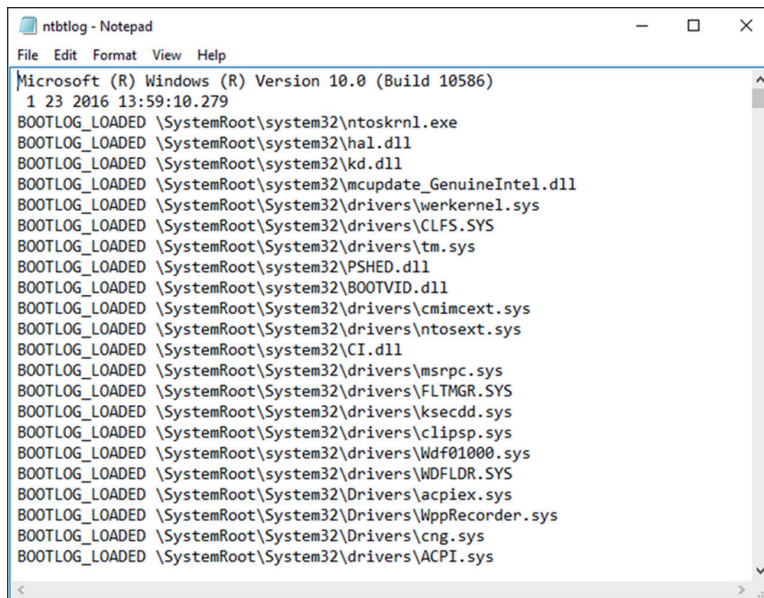
Don't restart your computer yet; you will do this as a part of the next exercise.

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 10 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 10.6.

FIGURE 10.6   A Windows 10 boot log file


```
ntbtlog - Notepad                                          —    □    ×
File  Edit  Format  View  Help
Microsoft (R) Windows (R) Version 10.0 (Build 10586)
 1 23 2016 13:59:10.279
BOOTLOG_LOADED \SystemRoot\system32\ntoskrnl.exe
BOOTLOG_LOADED \SystemRoot\system32\hal.dll
BOOTLOG_LOADED \SystemRoot\system32\kd.dll
BOOTLOG_LOADED \SystemRoot\system32\mcupdate_GenuineIntel.dll
BOOTLOG_LOADED \SystemRoot\System32\drivers\werkernel.sys
BOOTLOG_LOADED \SystemRoot\System32\drivers\CLFS.SYS
BOOTLOG_LOADED \SystemRoot\System32\drivers\tm.sys
BOOTLOG_LOADED \SystemRoot\system32\PSHED.dll
BOOTLOG_LOADED \SystemRoot\system32\BOOTVID.dll
BOOTLOG_LOADED \SystemRoot\System32\drivers\cmimcext.sys
BOOTLOG_LOADED \SystemRoot\System32\drivers\ntosext.sys
BOOTLOG_LOADED \SystemRoot\system32\CI.dll
BOOTLOG_LOADED \SystemRoot\System32\drivers\msrpc.sys
BOOTLOG_LOADED \SystemRoot\System32\drivers\FLTMGR.SYS
BOOTLOG_LOADED \SystemRoot\System32\drivers\ksecdd.sys
BOOTLOG_LOADED \SystemRoot\System32\drivers\clipsp.sys
BOOTLOG_LOADED \SystemRoot\system32\drivers\Wdf01000.sys
BOOTLOG_LOADED \SystemRoot\system32\drivers\WDFLDR.SYS
BOOTLOG_LOADED \SystemRoot\System32\Drivers\acpiex.sys
BOOTLOG_LOADED \SystemRoot\System32\Drivers\WppRecorder.sys
BOOTLOG_LOADED \SystemRoot\System32\Drivers\cng.sys
BOOTLOG_LOADED \SystemRoot\System32\drivers\ACPI.sys
```

In Exercise 10.2, you will examine the boot log file that was created by default during Exercise 10.1.

EXERCISE 10.2

Using Boot Logging

1. Click Windows Explorer (the folder icon on the taskbar) and browse to `C:\WINDOWS\Ntbtlog.txt`. Double-click this file.

2. Examine the contents of your boot log file.

3. Shut down your computer and restart it without using Advanced Boot Options.

> **NOTE** The boot log file is cumulative. Each time you boot to Safe Mode, you are writing to this file. This enables you to make changes, reboot, and see whether 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 (Enable Boot Logging).

Using Other Startup Setting Options

In this section, you will learn about additional Startup Settings menu modes. These include the following options:

1) Enable Debugging   This runs the Kernel Debugger, if it is installed. The Kernel Debugger is an advanced troubleshooting utility.

2) Enable Boot Logging   When you enable boot logging, a file is created called `Ntbtlog.txt`. This file lists all the drivers that are installed during startup and that might be useful for advanced troubleshooting.

3) Enable Low-Resolution Video   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 10 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.

> **NOTE** Safe Mode starts Windows 10 at a resolution of 800×600.

4) Enable Safe Mode   As explained previously, entering into Safe Mode allows the system to boot up with only the minimum drivers needed to make the system operate.

5) Enable 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.

6) Enable Safe Mode With Command Prompt   This starts the computer in Safe Mode, but after you log in to Windows 10, only a command prompt is displayed. This mode does not provide access to the desktop. Experienced troubleshooters use this mode.

7) Disable Driver Signature Enforcement   This allows drivers to be installed even if they do not contain valid signatures.

8) Disable Early Launch Anti-malware Protection   Windows 10 has a feature called Secure Boot. Secure Boot helps protect the Windows boot configuration and its components. Secure Boot also loads an Early Launch Anti-malware (ELAM) driver. Choosing this option disables the Early Launch Anti-malware driver.

9) Disable Automatic Restart After Failure   This 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, preventing you from accessing the desktop or any configuration options.

Press Enter to Return to Your Operating System   This boots the Windows 10 system 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 10 normally.

Launch Recovery Environment   The Windows 10 Recovery Environment (WinRE) is used to repair common causes of bootable operating systems problems. By default, WinRE is preloaded into the Windows 10 for Desktop editions (Home, Pro, Enterprise, and Education).

Understanding System Restore

System restores are actually a two-part process to make work. First in the Windows 10 operating system, you create system restore points. These are snapshots of the Windows 10 system so in the event that you need to revert to one of these snapshots, you can.

So after you create some system restore points, the System Restore option in the Advanced Options allows you to revert your PC to an earlier point in time. Restore points are generated when an administrator or user installs a new application, driver, Windows update, or when you manually create a restore point.

When you restore to a previous point, the user's personal files won't be affected, but restores do remove applications, drivers, and updates installed after the restore point was made.

To enable System Protection (needed to create restore points), in Control Panel, choose the System icon. When the System Properties window appears, choose the System Protection tab. Click the Configure button (see Figure 10.7) to turn System Protection on.

FIGURE 10.7   Configure button for System Protection
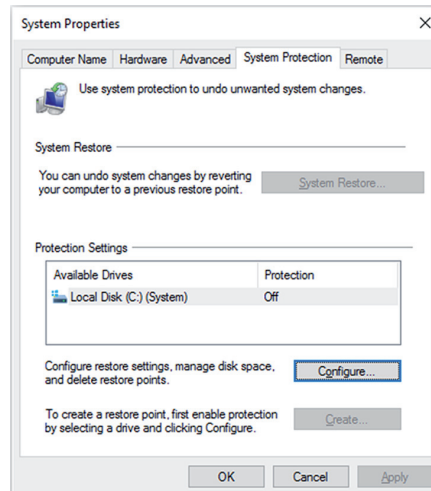
Once you have enabled System Protection in Control Panel, you then need to open the System Restore application. To do that, you follow these steps:

1. Right-click the Start button and then select Control Panel.

2. Choose Control Panel ➤ Recovery.

3. In the Recovery window, choose Configure System Restore (as shown in Figure 10.8).

FIGURE 10.8   Open System Restore
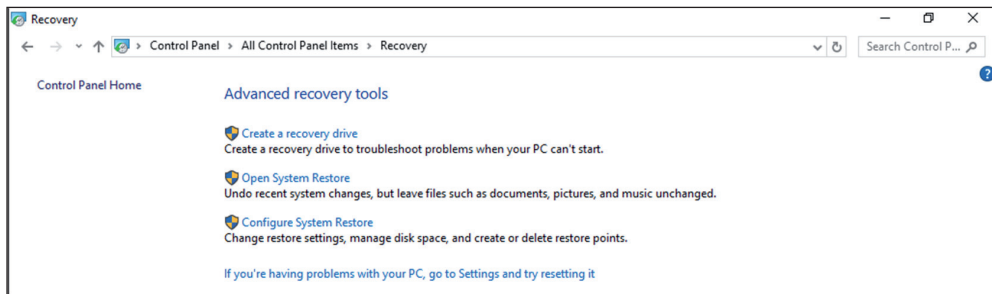
4. At the next screen, click the Create button. This will allow you to create a system restore point.

> **NOTE**   The steps to create restore points as well as restore and clean up old restore points will be explained in the section "Maintaining Windows 10 with Backup and Restore," later in this chapter.

Before you can use the system restore to fix a crashed computer, you need to create a recovery drive. Recovery drives allow you to create a backup drive in the event that a PC can't start. After the recovery drive is created, you can then use that drive to recover from a system crash.

To use the recovery drive to fix a crashed computer, boot the system into the Advanced options and then choose System Restore. Then it will ask you for a username and then a password and the system will continue using one of the restore points that was selected.

Using the System Image Recovery

Another way to protect your Windows 10 computer system is to create and use system images. System images are exact copies of the Windows 10 drive. System images, by default, include the drives that are needed for Windows to function properly. System images include Windows and all of the system settings, programs, and files.

System images work well in the event of a major hard disk or computer crash. System images allow you to restore all of the contents of the crashed system and get the system back up and running. When you restore a crashed system from an image, the entire system is restored. It's a complete restore of the computer system. This means that you can't pick and choose what programs you want to install. It's an all-or-nothing restore.

This is the reason why you should also make sure that you do regular backups. By making sure all of your backups are up to date and by making sure you have a system image, you are completely covered in the event of a major crash.

To create a system image, right-click the Start menu and choose Control Panel. In the Control Panel, open File History. Once you're in the File History application, click the System Image Backup link in the lower-left corner (see Figure 10.9).

FIGURE 10.9   System Image Backup
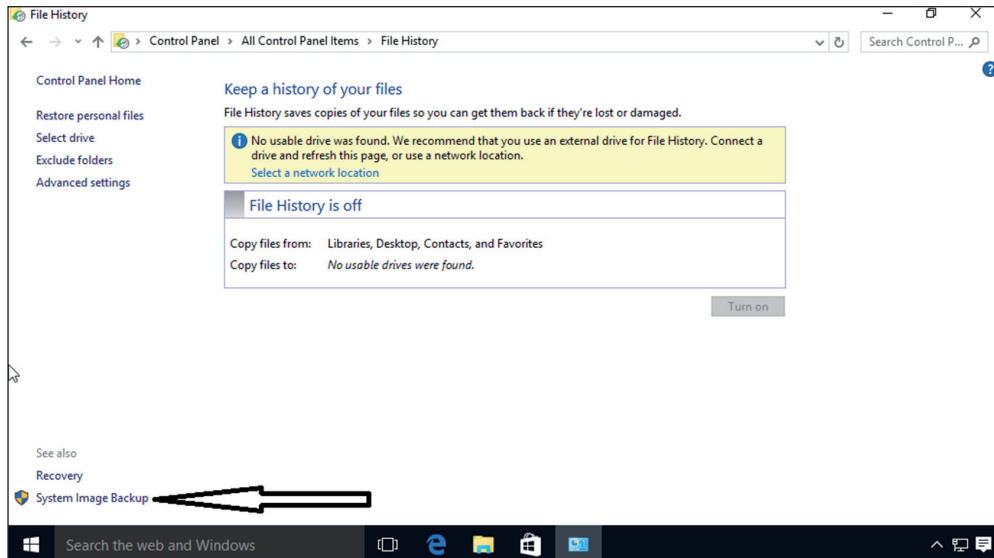
The steps to create a System Image Backup will be explained in "Maintaining Windows 10 with Backup and Restore."

Using the Startup Repair Tool

Another option that is available in the Advanced Options menu is the Startup Repair tool. If your Windows 10 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 utility discussed in the next section.

If Startup Repair is unable to correct the problem, you might have to reinstall Windows 10, but this should be done as a last resort. This is one reason why you should always back up your Windows 10 machine.

Maintaining Windows 10 with Backup and Restore

The Windows 10 *Backup and Restore utility* enables you to create and restore backups. Backups protect your data in the event of system failure by storing the data on another medium, such as a hard disk, CD, DVD, or network location. If your original data is lost because of corruption, deletion, or media failure, you can restore the data by using your backup.

To access Backup and Restore, type **backup and restore** in the Windows 10 search box. Alternatively, you can choose Start ➢ Control Panel, choose either the small or large icon view, and then click Backup And Restore (Windows 7). Backup and Restore is shown in Figure 10.10.

Creating a Backup

You can see in Figure 10.10 that no backups of this Windows 10 machine have been taken. To set up a backup, choose the Set Up Backup link in the right side of the Backup And Restore window. Choosing Set Up Backup launches a wizard that takes you through the process of creating a backup. The Backup Wizard first asks you for a location to save your backup. This location can be a hard disk (removable or fixed), a CD, a DVD, or even a network location (if you have Windows 10 Premium or Ultimate).

FIGURE 10.10 Windows 10 Backup and Restore
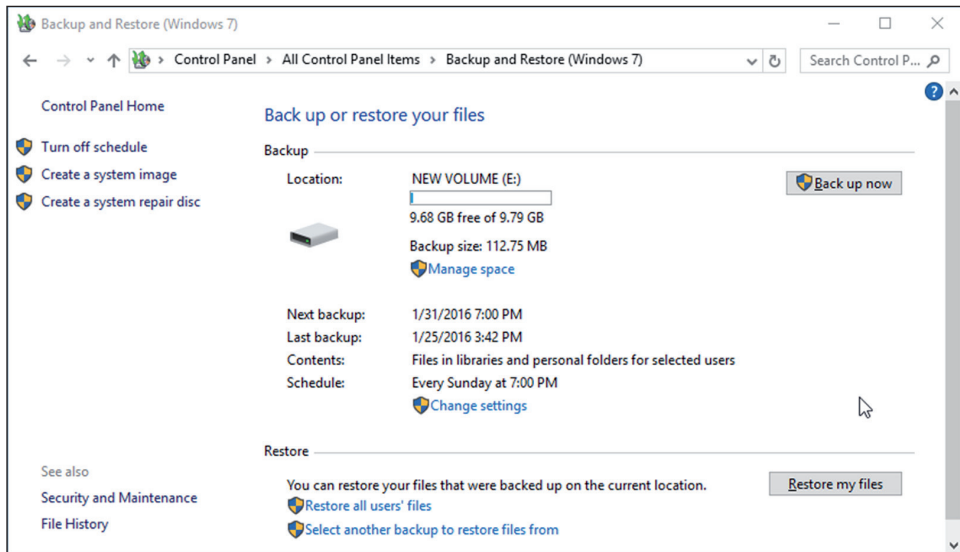
Next, you are asked to either let Windows 10 choose the files and folders to back up or let you manually select the resources you want to back up. In your manual selection, you can choose just the data libraries of Windows 10 for you as a user or other users. You can also choose to create a backup of the Windows 10 system files. If you want to choose other files and folders, you have the option of selecting any resources individually on your hard disk(s).

The final page of the wizard enables you to view the items you have selected as well as set up a schedule for your backups to occur. If you're happy with the setup, click the Save Settings And Run Backup button. The backup commences, and you are able to restore the resources if necessary in the future. Figure 10.11 shows my Windows 10 machine right after I chose to save the settings and run a backup. You can see the backup in progress and the date and time of my last backup.

> **NOTE** Windows 10 *cannot* back up encrypted files. To back up encrypted files, you need to manually copy all encrypted files to an external hard drive or decrypt the files before the backup.

In Exercise 10.3, you will make a backup of your files. This exercise assumes that you haven't yet configured an automatic backup.

FIGURE 10.11 Windows 10 backup status
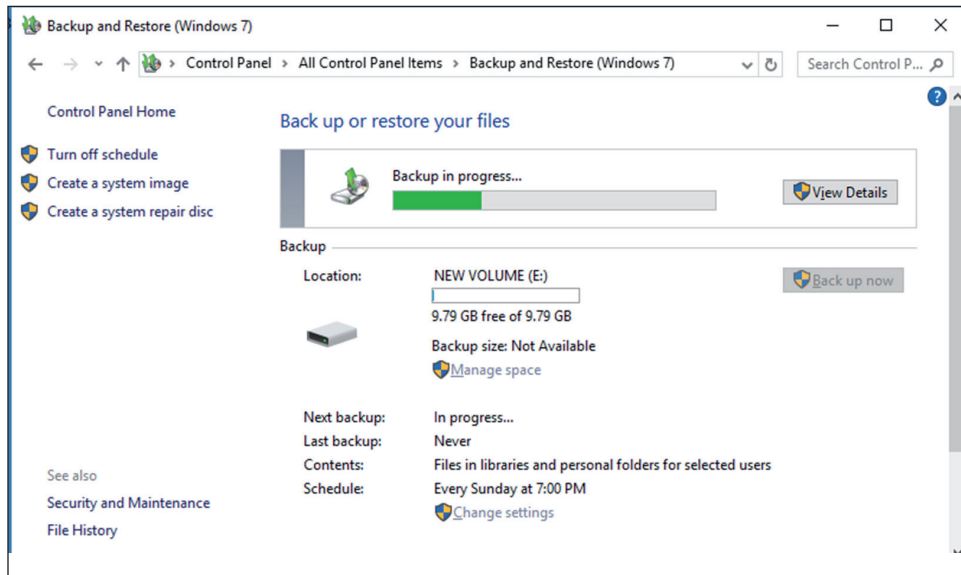
EXERCISE 10.3

Backing Up Files

1. Right-click Start ➢ Control Panel ➢ Backup And Restore (Windows 7).

2. Click the Back Up Now button.

3. Select the location where you want to save your backup, and then click Next. In our example, we will use our D: drive.

4. The What Do You Want To Back Up? screen appears. Click the Let Me Choose radio button and then click Next.

5. Select the files that you would like to back up. Click Next.

6. At the Review Your Backup Settings screen, you can select how often you want a backup to be automatically performed. To start the backup, click the Save Settings And Run Backup button.

   Windows begins backing up files, and a progress indicator indicates how the backup is progressing.

7. When the backup is complete, click Close.

After you have created your backup, you can restore system files and user data files with the Backup and Restore utility.

Restoring Files from a Backup

If you have lost or destroyed files that you still want on your Windows 10 system, you can restore them from your backup. To restore files to your computer, launch the Backup and Restore program by typing **backup and restore** in the Windows 10 search box. Assuming the media where your backup was saved is available, you can click the Restore My Files button.

Click the Restore My Files button to launch a restore wizard that prompts you to search for the files you want to restore. You can select multiple files and folders. When you have selected all the files and folders you want to restore, click Next, and you will have one final option: to restore to the original location or pick an alternative location for restoration. After you make the restore-location decision, choose Restore. The restore operation commences, and your original files and folders are available for you from the backup media.

You also have options in the Backup And Restore window to restore all users' files or to select another backup to restore files from. You would use this second option if you saved your backup to multiple locations and the last one (the one listed in the backup section) is not the set of backup files you want to use in your current session. Other than just restoring files and folders, you have the choice to use other advanced backup options.

In Exercise 10.4, you will restore some files. This exercise assumes that you created a backup in Exercise 10.3.

EXERCISE 10.4

Restoring Files

1. Right-click Start ➢ Control Panel ➢ Backup And Restore (Windows 7).

2. Click the Restore My Files button.

3. At the Restore Files screen, click the Browse For Folders button.

4. Click the Microsoft Windows Backup link in the left window. Then double-click the backup that you created in the previous exercise. Choose the folder that you want to restore (we chose the `Program Files` folder, but you need to choose a folder with enough free space) and click Add. Click Next to continue.

5. Select whether you want files saved in the original location or a different location. To begin the restore, click Restore.

6. When the restore is complete, click Finish.

Recovering Files from OneDrive

As explained in Chapter 3, "Configuring Storage and Security," Microsoft has a subscription-based storage system called OneDrive. Microsoft's OneDrive is built into Windows 10 by default. OneDrive is a cloud-based storage subscription so home users can store their documents and then access those documents from anywhere in the world (provided that you have Internet access).

OneDrive was designed for the average home user who is looking to store data in a safe, secure, cloud-based environment. OneDrive, when first released, was also a consideration for corporate environments, but with the release of Windows Azure, OneDrive is really intended for the home user or corporate user who wants to store some of their own personal documents in the cloud. Corporations would be more inclined to use Microsoft Azure and all of its corporate benefits.

Exercise 10.5 will show you how to set up a OneDrive account for your user account. To do this, you must have a Microsoft account. You get 5 GB for free from Microsoft on the OneDrive cloud-based storage.

> **NOTE** If you did Exercise 3.3 in Chapter 3, "Configuring Storage and Security," please skip the following exercise.

EXERCISE 10.5

Configuring OneDrive

1. Open OneDrive.

2. Log into OneDrive using your Microsoft account.

3. You will get a screen that shows where your files will be located on your system. Click the Next button.

4. At the Sync Files screen, choose what folders that you want to sync with Microsoft and then click Next.

   A screen will appear telling you that your OneDrive is set up and ready to go.

5. Click the Open My OneDrive Folder button to open your folders and Microsoft OneDrive.

6. Close OneDrive.

Now that the OneDrive subscription has been set up, you can recover files and folders from clicking Windows Explorer and then choosing OneDrive from the left side. You can recover any of the files and folders that were stored on OneDrive.

Using the Wbadmin Command Utility

Administrators have the ability to configure and manage backups and restores through the command prompt using a utility called Wbadmin. The Wbadmin.exe command replaces the Ntbackup.exe command that was released with previous versions of Windows. Wbadmin allows you to back up and restore your operating system, volumes, files, folders, and applications all from a command prompt.

You must be a member of the Administrators group to configure a regularly scheduled backup. To perform any other tasks using Wbadmin, you must be a member of either the Backup Operators group or the Administrators group, or you must have been delegated the appropriate permissions.

To run the Wbadmin.exe command, you must start it from an elevated command prompt. To do this, click Start, right-click the command prompt, and then click Run As Administrator.

Table 10.2 shows the Windows 10 Wbadmin command switches and their descriptions.

TABLE 10.2   Wbadmin switches

Command	Description
Wbadmin Start Backup	Runs a one-time backup
Wbadmin Stop job	Stops the currently running backup or recovery
Wbadmin get versions	Shows the details of a backup
Wbadmin get items	Lists items contained in a backup
Wbadmin get status	Shows the status of the currently running operation

Using Advanced Backup Options

In the main Backup And Restore window, you have options in the left pane to turn off the schedule, create a system image, and create a system repair disk.

Choosing the Turn Off Schedule option lets you take your backup out of the current backup scheduling as seen in Task Scheduler. Creating a system image lets you back up critical operating system files for restoration later if your operating system becomes corrupt. Creating a system repair disc allows you to create a bootable disc with which you will have a limited set of repair utilities and the ability to restore your backup files if necessary.

Creating a System Image

A *system image* enables you to take a snapshot of the entire hard disk and capture that image to a specific location so you can restore that image at a later date.

To create a system image of your entire computer, select the Create A System Image link on the left side of the Backup And Restore utility. When creating a system image, you can save that image to a hard disk, a DVD, or a network location.

In Exercise 10.6, you will create a system image and save it to a local hard disk.

Creating a System Image

1. Right-click Start ➢ Control Panel ➢ Backup And Restore (Windows 7).

2. Click the Create A System Image link on the left side.

3. Choose the location where you want to save the image. We are choosing the local D: drive. Click Next.

4. At the Confirm screen, click Start Backup.

5. A dialog box may appear, asking whether you want to create a system repair disc. Click the No button. If you want to create a system repair disc, you will need a DVD burner and DVD.

6. When the image is complete, click the Close button.

After you create a system image, you may need to restore it. Let's take a look at the steps needed to complete a restore.

Restoring an Image

When you need to restore an image, you will use the System Image Recovery tool. To restore an image using this tool, you must perform the following steps:

1. Boot your computer by using the Windows 10 media, or use the recovery partition instructions provided by your computer manufacturer.

2. When the Install Windows dialog box appears, select the language, the time and currency format, and the keyboard or input method. Click Next to continue.

3. The Install Now button appears 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 appears. You can choose one of the following options:

   - Startup Repair
   - System Restore
   - Windows Complete PC Restore
   - Windows Memory Diagnostic Tool
   - Command Prompt

   Choose Windows Complete PC Restore to continue.

6. Select the recommended image, or select Restore A Different Backup. Click Next to continue.

7. If you selected Restore A Different Backup, follow the prompts to select the location of the image and the image you want to restore.

8. You will be asked to review your selections. Click Finish to continue.

9. 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 10 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.

Using System Protection

System Protection is a feature of Windows 10 that creates a backup and saves the configuration information of your computer's system files and settings on a regular basis. System Protection saves multiple previous versions of saved configurations rather than just overwriting them. This makes it possible to return to multiple configurations in your Windows 10 history, known as *restore points*. These restore points are created before most significant events, such as installing a new driver. Restore points are also created automatically every seven days. System Protection is turned on by default in Windows 10 for any drive formatted with NTFS.

You manage System Protection and the restore points from the System Protection tab of the System Properties dialog box. You can also access this tab directly by typing **restore point** into the Windows 10 search box or by clicking the Recovery icon in Control Panel.

Clicking the System Restore button launches the System Restore Wizard, which walks you through the process of returning Windows 10 to a previous point in time.

Also within the System Protection tab of the System Properties dialog box is the Protection Settings section, where you can configure any of your available drives. Select the drive for which you would like to modify the configuration and click the Configure button. The System Protection configuration dialog box for the drive appears.

The System Protection dialog box allows you to enable or disable system protection for the drive. When you enable protection, you can opt for previous versions of files or previous versions of files and system settings. You also have the ability to set the maximum disk space that your restore points will use for storage. Another function of the System Protection dialog box for the selected disk is to delete all restore points (including system settings and previous versions of files) by clicking the Delete button.

One tool included with restore points is shadow copies. Shadow copies are copies of files and folders that Windows automatically saves as part of a restore point. Normally, restore points are made only once a day if you have enabled System Protection. If System

Protection is enabled, Windows will then automatically create shadow copies of files that have been modified since the last restore point was made.

One advantage of using restore points and shadow copies is the ability to restore files and folders using the Previous Versions tab. When you click any folder and choose Properties, the last tab on the right is Previous Versions. You can easily restore any folder by choosing one of these previous versions.

Creating Restore Points

Restore points contain Registry and system information as it was at a certain point in time. These restore points are created at the following times:

- Weekly
- Before installing applications or drivers
- Before significant system events
- Before System Restore is used to restore files (so you can undo the changes if necessary)
- Manually upon request

In Exercise 10.7, you will manually create a restore point.

EXERCISE 10.7

Creating a Restore Point

1. Right-click Start ➢ Control Panel ➢ System ➢ Advanced System Settings.

2. When the System Properties dialog box appears, click the System Protection tab.

3. Click the Create button on the bottom of the screen.

4. At the System Protection dialog box, enter a description for the restore point. Click Create.

5. A dialog box states that the restore point was created. Click Close.

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.

WARNING   System Restore will also remove any programs that have been installed since the restore point was created.

In Exercise 10.8, you will revert your system configuration to a previously captured restore point.

EXERCISE 10.8

Restoring a Restore Point

1. Right-click Start ➤ Control Panel ➤ System ➤ Advanced System Settings.

2. When the System Properties dialog box appears, click the System Protection tab.

3. Click the System Restore button. Click Next at the Welcome screen to continue.

4. Choose the restore point created in the previous exercise and click Next to continue.

5. Review your restore point selection, and click Finish to continue.

6. Click Yes to confirm that you want System Restore 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.

Cleaning Up Old Restore Points

One problem with creating multiple restore points is that they start to take up a large amount of your hard disk. You will need to clean up old restore points from time to time, and you can accomplish this task by using the Disk Cleanup utility.

The Disk Cleanup utility removes temporary files, empties the Recycle Bin, and removes a variety of system files and other items that you no longer need. When using the Disk Cleanup utility, you can also click the More Options tab and choose Programs And Features and System Restore And Shadow Copies to clean them up as well.

> **NOTE** The More Options tab is available when you choose to clean up files from all users on the computer.

To use the Disk Cleanup utility, right-click Start ➤ Control Panel ➤ Administrative Tools ➤ Disk Cleanup.

Using the Recycle Bin

Now we are going to talk about an icon that we have seen on our desktop for many years called the Recycle Bin. The Recycle Bin is a temporary storage container that holds deleted files. The advantage of have a temporary storage container is that you can restore or recycle the files to their original location. So basically it allows you to undelete a deleted file.

When a file or folder is deleted on a computer, it isn't actually deleted. When files or folders get deleted, they get placed into the Recycle Bin. This works well because if you change your mind or realize that you actually need the file or folder, you can undelete it

and it gets restored. The Recycle Bin allows you to perform a refresh or recycle of files that were deleted but shouldn't have been.

The Recycle Bin allows you to restore files or folders multiple ways. You can right-click the item and choose Restore or you can use the Manage tab (as shown in Figure 10.12).

FIGURE 10.12   Manage tab in Recycle Bin
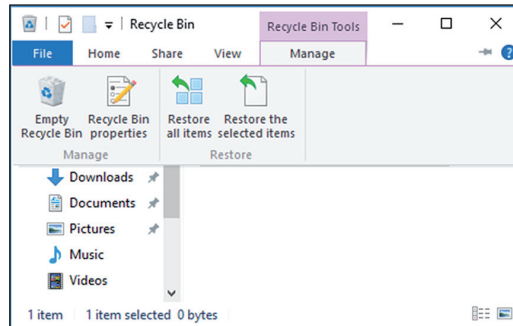
In Exercise 10.9, you will create a document and then delete the document. Then you will use the Recycle Bin to restore the document to its original location.

EXERCISE 10.9

Using the Recycle Bin

1. On the Windows 10 desktop, right-click and choose New Text Document.

2. Create a new test document called `Test.txt`.

3. After the document is created, right-click the document and choose Delete.

4. Double-click to open the Recycle Bin.

5. You can either right-click the `Test.txt` document and choose Restore, or click the document and then on the Manage tab choose Restore The Selected Item.

6. Close the Recycle Bin, and the document should be back on the desktop.

Summary

In this chapter, you looked at the different ways to recover and protect your Windows 10 machine from hardware and software issues. We discussed using the Advanced Boot Options such as Safe Mode, Debugging Mode, and VGA Mode.

Another important item that needs to be completed on a Windows 10 machine is Backup and Restore (Windows 7). Backing up a Windows 10 machine protects data in the event of a hardware or software failure.

We also discussed how to back up a complete copy of Windows 10 by using images. An image allows you to copy the entire Windows 10 machine and then reimage the machine in the event of a major failure. Another way to protect data is by the use of shadow copies. Shadow copies, which are a part of System Protection, allow you to keep previous versions of data and revert to that previous version in the event of a problem.

Video Resources

There are no videos for this chapter.

Exam Essentials

Understand the different options for managing system recovery.   Know how to use the Startup Repair tool, System Restore, and the Backup and Restore Center and when it is appropriate to use each option.

Be able to perform file recovery with the Backup and Restore Center and shadow copies.   Understand the options that are supported through the Backup and Restore (Windows 7) Center and the files that are backed up using this tool. Know how to manually create a shadow copy and how to keep only the last shadow copy version.

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 the difference between Last Known Good Configuration, Safe Mode, Debugging Mode, and VGA Mode.

Review Questions

1. You are the network administrator for a large organization that uses both Windows Server 2012 R2 and Windows 10. One of the Windows 10 machines needs to be backed up daily. You perform an image backup on the Windows 10 machine. The Windows 10 machine then gets struck by a virus and will not start up properly. What can you do to get the Windows 10 machine up and running the fastest possible way?

    A. Because of the virus, the best thing is to rebuild the machine from scratch.

    B. Start the computer from the Windows 10 DVD and then use the System Image Recovery tool.

    C. Start the computer from the Windows 10 DVD and then use the Image Restore utility.

    D. Use a Windows 10 boot disk and run the Image Restore utility.

2. You need to back up Windows 10, but the backup must be backed up to a local disk drive. When you start the backup, you see the screen shown in Figure 10.13.

    FIGURE 10.13 Backup and Restore (Windows 7) error
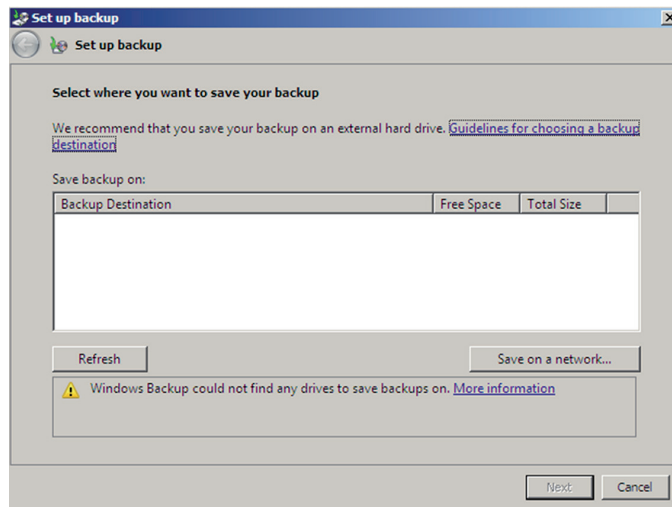
    What action do you need to perform?

    A. Log on as the backup administrator.

    B. Log on as the system administrator.

    C. Add a local hard disk to the machine by using Computer Management and then run the backup again.

    D. Run the backup utility in protected mode.

3. You are the system administrator for a large organization that uses Windows Server 2012 R2 and Windows 10. You have a Windows 10 machine and have enabled System Protection. You want the machine to retain only the last System Protection snapshot that was taken. What should you do?

   A. Run Disk Cleanup for System Restore and then run Shadow Copies.

   B. Disable Shadow Copies and run System Protection.

   C. Set the Keep Only Last Shadow Copy option in System Protection.

   D. Enable Shadow Copies and then set the Keep Only Last Shadow Copy option.

4. You are the network administrator for a small company. You manage the computers for the Marketing department, all of which are running the Windows 10 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

5. Your computer uses a SCSI adapter that supports a SCSI drive, which contains your Windows 10 system and boot partitions. After updating the SCSI driver, you restart your computer, but Windows 10 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 System Image reload.

   C. Boot your computer with the Safe Mode option and do a driver rollback.

   D. Boot your computer to the Recovery Console and manually copy the old driver back to the computer.

6. 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

7. After you updated Will'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 unable to boot your Windows 10 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.

9. You have been having problems with your Windows 10 computer. You decide to start the computer by 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`

10. You have purchased a new computer with Windows 10 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 by using the Back Up Files button in the Backup and Restore Center.

   B. Create an image of your computer by using the Create An Image link in the Backup and Restore Center.

   C. Use the System Repair tool to make an image of your computer.

   D. Use Shadow Copies to create a previous version of the files.

Appendix

Answers to the Review Questions

Chapter 1: Installing Windows 10

1. A. 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.

2. B. By modifying the changes on the local Group Policy, you can manually configure your Windows Update settings. You can automatically configure the Windows Update settings by creating a server-issued Group Policy Object (GPO).

3. C. 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. Loadstate.exe then deposits the information that is collected to a computer running a fresh copy of Windows 10.

4. B. Device Stage is part of the Windows 10 operating system family. Device Stage allows you to connect a compatible device to your PC and a picture of the device will appear. This allows you to easily share files between devices and computers.

5. C. With the Windows Hyper-V client, an organization that chooses to upgrade to Windows 10 will still have the ability to run older Windows XP applications on a virtual Windows XP system.

6. C. You can't upgrade Windows XP to Windows 10, so you must use a migration tool to migrate all the users' data and then install a clean copy of Windows 10.

7. D. The feature the question is referring to is View Available Networks (VAN). Before Windows 10, when you used a wireless network adapter, you would choose the wireless network that you wanted to connect to by using the wireless network adapter properties. In Windows 10, this is built into the operating system.

8. B. HomeGroup provides an easy way to set up a network using Windows 10. Windows 10 will search for your home network, and if it is found, it will connect after the HomeGroup password is entered. If a home network is not found, a networking wizard will automatically create a password for the HomeGroup so other computers can join.

9. B. Jump Lists is a feature in Windows 10 that allows you to quickly access files that you have been working on. Another advantage to using Jump Lists is that certain applications, such as Windows Media Player, can be preset, and in the case of Internet Explorer, you could view all the recent websites that you have visited.

10. C. Windows Touch allows you to control the operating system and its applications by using a touch screen. Touch screens can be placed on laptops, tabletops, GPS devices, phones, and now on the Windows 10 operating system.

Chapter 2: Automated Windows 10 Deployments

1. D. You would use the Sysprep utility. The `/generalize` options prevents system-specific information from being included in the image.

2. A. The DISM utility with the `/get-drivers` switch allows you to find out which drivers are installed on the WIM.

3. 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, and you can set them using WDSUTIL.

4. C. Windows System Image Manager (SIM) is used to create unattended answer files in Windows 10. 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. Image Capture Wizard 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` option prevents system-specific information from being 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.

Chapter 3: Configuring Storage and Security

1. D. Both Windows 10 and Windows XP Professional support FAT32 and NTFS, so both file systems will be viewable on both operating systems.

2. A. In Windows 10, it is possible to share encrypted files with another person or between computers. To share encrypted files, you must have a valid EFS certificate for the user who should have access to the files.

3. C. Windows 10 supports mirrored volumes, which allow you to have fault tolerance in the event of a single hard-disk failure.

4. D. Dynamic disks are supported by all Windows operating systems above Windows Server 2000. Windows 10 supports mirrored volumes.

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.

6. D. In Windows 10, one way you can compress files is through Windows Explorer. Windows 10 has no programs called Packer, and JetPack is for compressing JET databases. The Cipher program is used to encrypt or decrypt files. The command-line option for managing file and folder compression is Compact.

7. B. The Cipher utility is used to encrypt or decrypt files. Windows 10 doesn't have a program called Encrypt, Crypto, or EDS. If you want to manage file encryption through a GUI utility, you can use Windows Explorer.

8. D. Windows 10 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. C. To allow Tylor to access her encrypted files, Julie should import Tylor's encryption key and then add that key to each file to which Tylor 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 emailing Julie's key to Tylor will not allow Tylor to access the file.

10. B. You can increase the level of security on folders and files on an NTFS partition by using 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.

Chapter 4: Managing Data Access

1. B, C. Create a new HomeGroup and set the password. Use that password and join all computers to the same HomeGroup. By default, all files in the HomeGroup libraries are available to all members of the HomeGroup.

2. D. Windows 10 come with a feature called BitLocker Drive Encryption. BitLocker encrypts the entire system drive. New files added to this drive are encrypted automatically. To configure BitLocker, you must either use a Local Group Policy or use the BitLocker icon in Control Panel.

3. A, C, D. BitLocker Drive Encryption is a data protection feature available in Windows Education, Enterprise, and Professional editions of Windows 10.

4. 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.

5. A. The easiest way to manage this transition is to simply rename Rick's account to John. It is very important to remember that rights and permissions get associated to a user's SID number and not a username. By renaming Rick's account to John, John will automatically have all of the rights and permissions to any resource that Rick had access to.

6. E. By giving Tom Modify on the NTFS security setting, you're giving him just enough to do his job. You could also give Sales or Finance the Modify permission, but then everyone in those groups would be able to delete, change, and do more than they all need. Also, Tom does not need Full Control to change or delete files.

7. C, E. The Admin group needs Full Control on the NTFS security and shared permission settings in order to do their job. To be able to give other users permissions, you must have the Full Control permission.

8. D. Smart cards are plastic cards (the size of a credit card) that can be used in combination with other methods of authentication. This process of using a smart card along with another authentication method is called two-factor authentication or multifactor authentication.

9. A. File extensions for known files are hidden by default. If you want to be able to see the file extension for all files, you must uncheck the Hide Extensions For Known File Types box.

10. B. Microsoft BitLocker Administration and Monitoring (MBAM) will allow the IT department to use enterprise-based utilities for managing and maintaining BitLocker and BitLocker To Go.

Chapter 5: Managing the Windows 10 Environment

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, C. In Windows 10, you can edit the Registry with REGEDIT or REGEDT32. You should always use extreme caution when editing the Registry because improper configurations can cause the computer to fail to boot.

3. A. You configure keyboard and mouse properties in Control Panel.

4. C. On a laptop computer, Denise can use the battery meter to view the amount of battery power available and to change the power plan configured for the computer.

5. 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.

6. D. When the computer enters sleep mode, the data will be saved to memory, and the computer will be put into a power-saving state. Sleep mode combines the features of standby and hibernation so that all data is saved, but the computer restores faster than if the computer was put into hibernation mode.

7. A. You should use the Windows ReadyDrive technology to help speed the resume time of your computer after it has been put into hibernation 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 hibernation mode.

8. C. When a Windows 10 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.

9. A. The easiest way to configure the Desktop is by right-clicking an open area of the desktop and choosing Personalize.

10. 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.

Chapter 6: Planning and Managing Microsoft Intune

1. A. Administrators have the ability to limit and monitor network usage by configuring the network as a metered network. Network metering allows network downloading to be watched or metered, and then administrators can charge users or departments for the network usage.

2. D. Microsoft Intune does not allow you to change a security group parent. When you delete a group, the users are not deleted, and the only way to change a group's parent group is to create the security group under the parent. So, Portsmouth needs to be re-created under NHGroup, and then the users need to be re-added to Portsmouth.

3. C, D. As long as the salesperson's personally owned Windows 10 laptop is being managed by the management infrastructure agent, administrators can use remote wipe feature. When you do a remote wipe, all of the company's data gets wiped from the device.

4. D. An Apple Push Notification service (APNs) certificate must be imported from Apple so that the school can manage iOS devices. This certificate allows Intune administrators to manage iOS.

5. A. To configure the update restart prompt setting, you must configure the Microsoft Intune Agent Settings policy. Setting the "Prompt user to restart Windows during Intune client agent mandatory updates" to No, this would stop users from receiving restart prompts after mandatory updates.

6. C, D. If using Configuration Manger, administrators must configure Configuration Manager to manage mobile devices. To do this, it requires administrators to create a Windows Intune subscription and use a connector to synchronize user accounts.

7. B. Administrators can have the cloud-based version of Active Directory (Azure Active Directory) work with the on-premise server-based version of Active Directory by using the Azure Active Directory (AD) Connect tool (formerly known as the Directory Synchronization tool, the Directory Sync tool, or the DirSync.exe tool).

8. C. By default, licensed users can add up to five devices to their accounts. Device Administrators have the ability to add devices to Intune, but users do have the ability to enroll five devices on their own.

9. D. Sideloading an application means that you are loading an application that you already own or one that your company created into a delivery system (i.e., Intune, Microsoft Store, or images).

10. B, C. Intune administrators have the ability to set up different notifications to different emails based on alert type. So, you can send all alerts, critical alerts, warnings, and informational alerts to different IT members.

Chapter 7: Configuring Applications

1. A. The disconnected operation mode allows App-V Desktop Clients to run applications even when the client cannot connect to the App-V Management Server. This allows laptops to continue to access App-V applications even when not connected to the network or Internet. To stop that from happening, you must disable the disconnected operation mode.

2. A. The Default Programs icon in Control Panel allows you to set file extension associations to the various programs in Windows 10.

3. B. An InPrivate session prevents the browsing history from being recorded and does not allow temporary Internet files to be retained. Cookies, usernames, passwords, and form data will not remain in IE11 and Edge following the closing of the InPrivate session, nor will there be any footprints or data pertaining to the InPrivate browsing session.

4. B. Because all users and computers are part of the domain and the internal website uses Integrated Windows Authentication, once you add the URL to the Local Intranet zone properties, Windows Authentication will take over.

5. B. Shared computer activation (SharedComputerLicensing) allows an administrator to set up Office 365 ProPlus on a single computer for multiple users.

6. C. Administrators can test AppLocker policies before implementing them by using the audit-only mode.

7. C. The Azure Active Directory Module for PowerShell Set-Mailbox cmdlet allows you to manipulate an Office 365 mailbox.

8. A. Administrators can use PowerShell Direct to run PowerShell commands on a VM from the Hyper-V host. To do this, you need to run Invoke-Command and specify which VM you're connecting to (i.e., the VMName parameter).

9. C. AppLocker is a feature included with Windows (Windows 7 and higher) that allows administrators to lock out certain applications from running.

10. B. Applications that are developed by a company and are not signed by the Windows Store can be installed by the process of sideloading. Sideloading allows a company to load applications into the Windows Store for deployment throughout the company.

Chapter 8: Managing Identity and Authorization

1. A, D. The password aBcdEfG1! meets complexity requirements because it is at least six characters long and contains an uppercase letter, lowercase letters, and a symbol. The password 123456789nA meets complexity requirements because it is at least six characters long and contains an uppercase letter, a lowercase letter, and numbers. Complex passwords must be at least six characters long and contain three of the four types of characters—uppercase letters, lowercase letters, numbers, and symbols.

2. A. You do not want this user to have any administrator rights. To allow this user to change Windows Update manually, you must set this in an LGPO.

3. B. Application Control Policy (AppLocker) allows you to configure a Denied list and an Accepted list for applications or users. Applications that are configured on the Denied list will not run on the system or cannot be run by specific groups, and applications on the Accepted list will operate properly.

4. D. LGPOs are policies that you can set on a local Windows 10 machine to limit hardware and user usage. You also have the ability to control individual users within the Local Group Policy.

5. B. Audit Object Access enables auditing of access to files, folders, and printers.

6. 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.

7. D. Windows 10 comes with a new feature called BitLocker Drive Encryption. BitLocker encrypts the entire system drive. New files added to this drive are encrypted automatically. To configure BitLocker, you must either use a Local Group Policy or use the BitLocker icon in Control Panel.

8. A, B, C, D. UAC is available in all Windows 10 editions.

9. 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.

10. B. Account Lockout Policy, a subset of Account Policies, 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.

Chapter 9: Configuring Network Connectivity

1. C. Subscribing to Azure Active Directory allows a small to midsize company to have Active Directory without the need of purchasing new hardware.

2. A, B. You can see what the IPv6 address is by clicking the Details button from the network connection status or by typing **`ipconfig /all`**. There is no such command as `ipconfig /view`, and the My Computer properties will not show IP address configuration information.

3. B, C. Create a new HomeGroup and set the password. Use that password and join all computers to the same HomeGroup. By putting all files in the media library, they will be available to all members of the HomeGroup.

4. C. The company's subnet mask is 255.255.224.0. This subnet mask uses subnet ranges of 32. So, the subnet's layout is 32–63, 64–95, 96–127, 128–159, 160–191, and 192–223. Now when you subnet, you can't use the first or last number of any range. The first number represents the network ID, and the last number represents the broadcast. Because the router and the one Windows 10 computer fall within the 32–63 range, your new Windows 10 machine must fall within this range. 32 is the network ID and can't be used, and 63 is the broadcast and can't be used. So, the only available addresses are from 33–62, and the only available unused IP address in that range is 192.168.2.41.

5. A. Stateful is what we currently do today with IPv4. Stateful means that DHCP is going to give our IPv6 clients all of their TCP/IP data (IP address, default gateway, and all DHCP

options). Stateless configuration means that the clients address is based on the router's advertisement messages. Clients create their own IP address and default gateway based on the router's advertisement message and their MAC address. They can still get all of the other DHCP options, but they will not get an IP address and default gateway from DHCP.

6. B. You need to change the wireless network connection settings on the laptop to allow these laptop users to connect to the reconfigured access point.

7. C. `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.

8. B. When it comes to WPA, there are two versions: WPA2-Personal and WPA2-Enterprise. WPA2-Personal allows you to set up WPA2 by using a shared password key. WPA2-Enterprise allows you to set up WPA2 by using a server for verification. Because all users are using AES with no shared password key, WPA2-Enterprise is the setting that you would choose.

9. C. ISATAP is the automatic tunnel addressing protocol providing IPv6 addresses based on the IPv4 address of the end interface (node). The IPv6 address is automatically configured on the local device, and the dual-stack machine can use either its IPv4 or IPv6 address to communicate on the local network.

10. C. On a 240 subnet mask, the ranges go by 16. Because this is a Class C, the ranges would be 16–31, 32–47, 48–63, 64–79, 80–95, 96–111, 112–127, 128-143, 144–159, 160–175, 176–191, 192–207, 208–223, and 224–239. Remember that in a Class C address, these are not all usable. You have to subtract the first number (network ID) and the last number (broadcast).

Chapter 10: Configuring Recovery

1. B. After starting the machine with the Windows 10 DVD, you can use the System Image Recovery tool to reload the backup image that you created.

2. C. When you are using the backup utility and no local disks are present, you must either configure an installed disk or physically install a hard disk before running the backup utility.

3. A. You have to run the Disk Cleanup utility to delete the previous versions and then run Shadow Copies in System Protection. There is no Keep Only Last Shadow Copy option.

4. 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.

5. C. If you need to get a stalled computer up and running as quickly as possible, you should start with the Driver Rollback option. This option is used when you've made changes to your computer's hardware drivers and now you have issues.

6.   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.

7.   C. To quickly repair the system files, you can use the Startup Repair tool. You can restore an image by 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.   B. When you run your computer in Safe Mode, you simplify your Windows 10 configuration. Only the drivers that are needed to get the computer up and running are loaded.

9.   A. When you enable boot logging, the file created is `\Windows\ntbtlog.txt`. This log file is used to troubleshoot the boot process.

10. B. You should create an image of your computer by using the Create An Image link in the Backup and Restore Center. Images back up everything on your computer. File backups cannot be used to back up system files and settings.

Index

E

M

O

Q

Comprehensive Online Learning Environment

Register on Sybex.com to gain access to the comprehensive online interactive learning environment and test bank to help you study for your MCSA Windows 10 certification.

The online test bank includes:

- **Assessment Test** to help you focus your study to specific objectives
- **Chapter Tests** to reinforce what you've learned
- **Practice Exams** to test your knowledge of the material
- **Digital Flashcards** to reinforce your learning and provide last-minute test prep before the exam
- **Searchable Glossary** to define the key terms you'll need to know for the exam
- **Videos** to guide you through chapter exercises

Go to `www.wiley.com/go/sybextestprep` **to register and gain access to this comprehensive study tool package.**

SYBEX®

A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.