Microsoft Technology Associate Series

# Windows Operating System Fundamentals

**COURSEWARE** 8369–1 **EXAM** 98–349

Microsoft Technology Associate

**Approved Courseware**

September 2012

Microsoft Technology Associate Series

CCI Learning Solutions Inc.

**Windows Operating System Fundamentals**

**Developers: Kenny Lee, Irina Heer**

**Publishers: Kelly Hegedus, Kevin Yulo**

This courseware is one in a series prepared by CCI Learning Solutions Inc. for use by students and instructors in courses on computer software applications. CCI designed these materials to assist students and instructors in making the learning process both effective and enjoyable.



The information in this courseware is distributed on an "as is" basis, without warranty. While every precaution has been taken in the preparation of this courseware, neither the author nor CCI Learning Solutions Inc. shall have any liability to any person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by the instructions contained in this courseware or by the computer software and hardware products described therein.

CCI Learning Solutions Inc. would like to acknowledge the financial support of the Government of Canada through the Canada Book Fund for our publishing activities.

CCI Learning Solutions Inc. is independent from Microsoft Corporation, and not affiliated with Microsoft in any manner. While this publication may be used in assisting individuals to prepare for a Microsoft Business Certification exam, Microsoft, its designated program administrator, and CCI Learning Solutions Inc. do not warrant that use of this publication will ensure passing a Microsoft Business Certification exam.

 **ISBN: 978-1-55332-339-6** **Printed in Canada**

# Working With the Data Files

The exercises in this courseware require you to use the data files provided for the book. Follow the instructions shown to download the data files for this courseware.

1. Launch your browser and navigate to the CCI Web site location http://www.ccilearning.com/data.
2. Enter: 8369 in the **Courseware #** box and click Find Data.
3. Select the *8369-1-student-data.exe* file then click **Run**. Click **Run** again in the Internet Explorer – Security Warning window, if necessary.
4. In the WinZip **Self-Extractor** dialog box, use the **Browse** button to specify the Windows Desktop as the location to unzip the file and then click **Unzip**.
5. The **8369 Student Files** folder containing the required student work files has now been downloaded to your desktop. It is recommended that you rename the folder using your own name before starting the exercises in this courseware. You can reinstall and use the work files as many times as you like.

# What is the Microsoft Technology Associate Certification?

The Microsoft Technology Associate (MTA) certification validates fundamental technology knowledge, allows you to explore possible career paths, and helps prepare you for advanced studies and certifications. You can choose which exam(s) you want to take according to which knowledge area(s) you want to validate. Some of the benefits of MTA Certification include:

Build a foundation for a technology career

Validate fundamental knowledge with an official Microsoft certification

Explore different career paths

Get access to the Microsoft Certified Professional (MCP) online community

Get an edge for college admissions or prepare for internships and entry-level jobs

Earn a Microsoft certification right in the classroom.*

The currently available Microsoft Technology Associate exams include*:

- Software Developer Fundamentals
- Windows Developer Fundamentals
- Web Developer Fundamentals
- Database Administration Fundamentals
- Windows Server Administration Fundamentals
- Networking Fundamentals
- Security Fundamentals

# What does the Microsoft Technology Associate Approved Courseware logo represent?

Approved Courseware

The logo indicates that this courseware has been approved by Microsoft to cover the course objectives that will be included in the relevant exam. It also means that after utilizing this courseware, you will be better prepared to pass the exam required to become a certified Microsoft Technology Associate.

## For more information:

To learn more about Microsoft Technology Associate exams, visit http://www.microsoft.com/learning/en/us/certification/mta.aspx

To learn about other Microsoft approved courseware from CCI Learning Solutions Inc., visit www.ccilearning.com/mta

* The availability of Microsoft Technology Associate certification exams varies by Microsoft program, program version and language. MTA exams are only available at academic institutions that have purchased an MTA Campus License or MTA vouchers. Contact your school administrator to find out if your school is an approved MTA testing center. Visit www.certiport.com/mta for exam availability.

# Table of Contents

## About This Courseware



## Lesson 1: Introduction to the Operating System



## Lesson 2: Operating System Configuration

## Lesson 3: Managing Users and Applications



## Lesson 4: Working with File Systems

## Lesson 5: Managing Different Devices



## Lesson 6: Maintaining Your System

# Appendices

# Course Description

*Windows Operating System Fundamentals* provides students with fundamental operating system configuration and administration concepts. Students who complete this course will have reviewed all of the exam objectives and be on their way to preparing for Microsoft Technology Associate Exam #98-349. It can also serve as a stepping stone to the Microsoft Certified Technology Specialist exams.

## Course Series

This *Windows Operating System Fundamentals* courseware is one in the Microsoft Technology Associate Series. Other courses available in the series include:

- Software Development Fundamentals
- Database Administration Fundamentals
- Networking Fundamentals
- Windows Development Fundamentals
- Web Development Fundamentals
- Security Fundamentals
- Windows Server Administration Fundamentals

The Microsoft Technology Associate Series contains exercises that students can use to learn each of the features discussed. Additional resources to practice and apply the skill sets are available from the CCI Technology Associate Microsite. Students are encouraged to register at http://mta.ccilearning.com in order access these additional activities both during and after completing the course.

Instructor Resources are available and are produced specifically to help and assist an instructor in preparing to deliver the course using the CCI materials. Contact your coordinator or administrator, or call your CCI Account Manager for information on how to access these resources.

## Course Prerequisites

Prior to taking this course, students must possess the following basic computer literacy and Windows skills.

- Start and run Windows
- Use Minimize, Restore Down/Maximize, or Close
- Use the left and right mouse buttons appropriately
- Understand file management techniques
- Navigate between files, folders, or drives

## System Requirements

**Supported Architecture**

- x86 or x64
- Single processor, 2 GHz or faster
- 1 GB RAM or higher

**Supported Operating Systems** (Note: This course was developed using Windows 7 Professional)

- Any version of Windows 7.
- The system must have TCP/IP installed and configured as the default networking protocol. If you use a standard installation of Windows 7, TCP will be properly installed and configured.

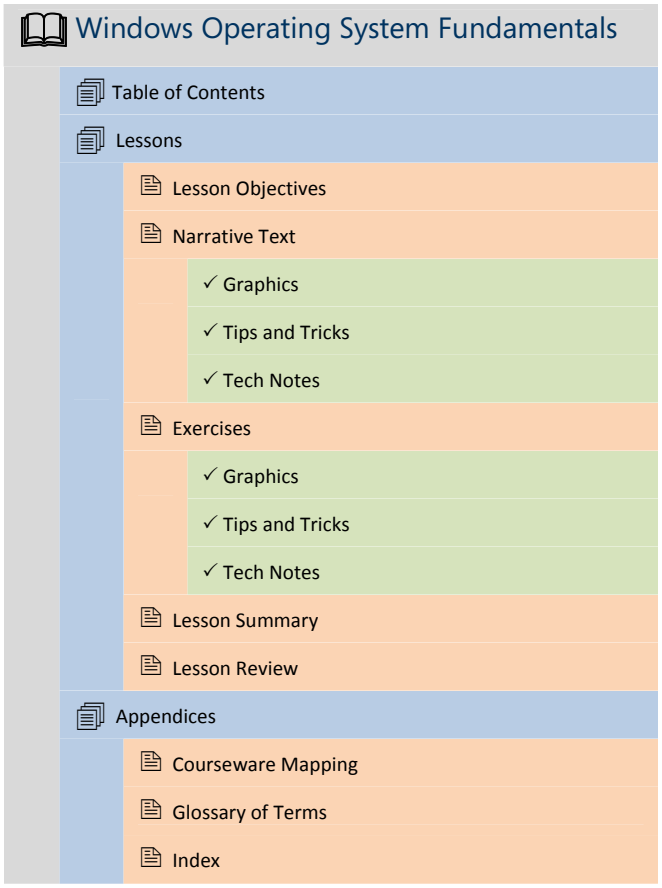
**Computer Setup:**

- Computers may be configured as part of a workgroup or as part of a domain.
- Each computer should be configured to participate in a LAN within the classroom.
- Each computer should be configured as a DHCP client.
- Each computer should have Internet access. Internet access is required for completing exercises involving Internet research.

# Course Design

This course book was developed for instructor-led training and will assist you during class. Together with comprehensive instructional text and objectives checklists, this course book provides easy-to-follow hands-on lab exercises and a glossary of course-specific terms.

This course book is organized in the following manner:




When you return to your home or office, you will find this course book to be a valuable resource for reviewing exercises and applying the skills you have learned. Each lesson concludes with questions that review the material. Lesson review questions are provided as a study resource only and in no way guarantee a passing score on a certification exam. Appendixes in the back of this course book provide additional information, resources, and answers to review questions.

# Course Objectives

After completing this course, you will be able to:

- Explain the difference between 32-bit and 64-bit operating systems.
- Describe the Windows 7 operating system editions, including features, availability and minimum requirements.
- Identify upgrade paths from various versions of Windows to Windows 7.
- Explain the function and characteristics of Windows Anytime Upgrade.
- Understand hardware and software compatibility issues and explain why upgrading to Windows 7 requires planning.
- Use the PC Upgrade Advisor.
- Use the Windows 7 Compatibility Center to check for software and hardware compatibility issues.
- Explain the difference between an in-place upgrade and a clean install.
- Explain different types of installation strategies, including High Touch installation, High Touch with Standard Image, Lite Touch installation and Zero Touch installation.
- Understand media-based and network-based installations.

- Explain cloud-based software deployment.
- Explain the purpose and advantages of virtualization.
- Explain the function and characteristics of Windows XP Mode.
- Explain the function and characteristics of MED-V.
- Identify the features and components of the Windows 7 Desktop.
- Understand how to navigate a breadcrumb trail.
- Identify the features and components of the Windows Explorer window.
- Add and configure Desktop gadgets.
- Describe and access user profile folders.
- Configure display settings, including screen resolution and screen magnification and configure Windows 7 to support multiple display devices.
- Create and modify Desktop shortcuts, create Start menu shortcuts, and add system icons to the Desktop.
- Use Aero features for window management.
- Modify and apply Aero themes.
- Use the Snipping Tool.
- Describe the major features of Internet Explorer.
- Describe the Windows Media Center.
- Describe Windows Media Player.
- Configure administrative tools.
- Configure accessibility options.
- Describe how to use MSCONFIG.
- Explain the Windows Sync Center.
- Explain the Windows Mobility Center.
- Explain administrator and standard user accounts.
- Describe the function of the User Account Control feature and describe its prompts and elevation levels.
- Describe the process of local, network, and group policy application installation.
- Install and remove application software.
- Describe the function and characteristics of services, and identify startup types, service accounts and service dependencies.
- Describe the advantages provided by remote management tools.
- Explain the Microsoft Management Console (MMC) and create a custom console.
- Explain how group policy is useful for remote management.
- Describe Windows PowerShell.
- Describe the function of Remote Desktop and explain the necessary configuration settings and underlying technologies.
- Explain application virtualization and describe the features and functions of App-V, Remote Desktop Services, and RemoteApp.
- Explain Virtual Desktop Infrastructure (VDI).
- Explain disk partitions and logical drives.
- Describe the file systems supported in Windows 7, including FAT32 and NTFS.
- Describe how to format a drive and how to convert a drive from FAT32 to NTFS.
- Explain the purpose and function of HomeGroups and describe how to create and join them.
- Describe public shares, basic shares and advanced shares.
- Explain how to map network shares to drive letters.
- Describe share permissions, NTFS permissions and effective permissions.
- Explain how to share printers.
- Explain basic encryption concepts.
- Describe the function of Encrypting File System (EFS) and BitLocker, and describe how to manage encryption keys.
- Explain disk compression.
- Explain the function and characteristics of libraries and describe how to use, customize, create and delete libraries.
- Explain the purpose and function of device drivers.
- Describe how compatibility issues between drivers and the operating system can affect the system.

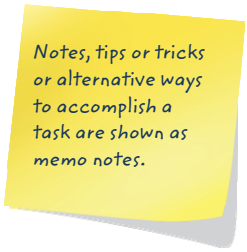
- Describe how and when to update device drivers.
- Explain system resources and resource allocation.
- Explain the features and function of Plug-and-Play technology.
- Explain when to install third-party software for devices.
- Describe storage device interfaces.
- Describe the function of RAID.
- Describe basic, dynamic and virtual hard disks.
- Describe the process of using cloud storage.
- Describe printer ports, printer drivers, the Print Spooler, and the Print queue.
- Compare and contrast local printers and network printers.
- Use the Devices and Printers page.
- Explain how to connect and share a local printer.
- Explain how to connect to a shared printer.
- Explain how to disconnect printers.
- Describe how to manage printers.
- Explain the purpose and function of the Microsoft XPS Document Writer.
- Describe how printing over the Internet works.
- Explain video, audio, and infrared devices.
- Describe how to use Windows Device Manager.
- Identify various types of malware.
- Identify security risks other than malware.
- Explain how malware affects the Windows Registry.
- Explain the use of firewalls.
- Describe the function and purpose of anti-spyware software.
- Describe the function and purpose of antivirus software.
- Describe how to avoid malware infection.
- Understand the function of the Windows Action Center.
- Explain and use the Malicious Software Removal Tool.
- Describe and use Windows Defender.
- Describe the function of Microsoft Security Essentials.
- Describe the function of Microsoft Forefront Endpoint Protection.
- Explain Windows Backup and Restore.
- Describe the function of system images.
- Describe the function of restore points.
- Describe the function of previous versions.
- Explain Advanced Boot Options, including Safe Mode and Last Known Good Configuration.
- Describe Microsoft update types.
- Explain how to use Windows Updates.
- Explain and use Windows system maintenance tools, including Defrag and Disk Cleanup.
- Explain how to use the Task Scheduler.
- Describe the purpose and function of the System Information tool.

# Conventions and Graphics

The following conventions are used in CCI learning materials.

| | |
|---|---|
| **File Names or Database Field Names** | File names or database field names are indicated in *italic* font style. |
| **Exercise Text** | Content to be entered by the student during an exercise appears in `Consolas` font. |
| **Procedures** | Procedures and commands you are instructed to activate are indicated in **bold** font style. |
| **Features or Command Options** | Menu options and features are listed in the left hand column and corresponding descriptions are in the right hand column. |

The following graphics are used in CCI learning materials.




Technical Notes point out exceptions or special circumstances that you may find when working with a particular procedure, or may indicate there is another method to complete the task.


Whenever you see this icon, navigate to http://mta.ccilearning.com for **M**ore **M**aterials on the **M**icrosite. These additional activities include online exercises and additional review. Use the microsite in class or at home to practice some of the skills you are having trouble mastering, or to try your skills using different materials.


This icon indicates the numbered objective from the Microsoft Technology Associate exam being covered in this topic. Refer to the Appendix for a complete listing of exam objectives.

**This symbol signifies the start of a step-by-step exercise**

# Lesson 1: Introduction to the Operating System

## Lesson Objectives

In this lesson, you will learn about the importance of selecting a suitable operating system for your home or organization, and about the wide variety of Windows 7 editions and installation options available. You will also learn how virtualization can allow an organization to upgrade to Windows 7 and still support legacy applications. By the completion of this lesson, you will be able to:

- ☐ Explain the difference between 32-bit and 64-bit operating systems.
- ☐ Describe the Windows 7 operating system editions, including features, availability and minimum requirements.
- ☐ Identify upgrade paths from various versions of Windows to Windows 7.
- ☐ Explain the function and characteristics of Windows Anytime Upgrade.
- ☐ Understand hardware and software compatibility issues and explain why upgrading to Windows 7 requires planning.
- ☐ Use the PC Upgrade Advisor.
- ☐ Use the Windows 7 Compatibility Center to check for software and hardware compatibility issues.
- ☐ Explain the difference between an in-place upgrade and a clean install.
- ☐ Explain different types of installation strategies, including High Touch installation, High Touch with Standard Image, Lite Touch installation and Zero Touch installation.
- ☐ Understand media-based and network-based installations.
- ☐ Explain cloud-based software deployment.
- ☐ Explain the purpose and advantages of virtualization.
- ☐ Explain the function and characteristics of Windows XP Mode.
- ☐ Explain the function and characteristics of MED-V.

### Exam Objectives

2.1 Identify Windows operating system editions
2.2 Identify upgrade paths
2.3 Understand installation types
2.4 Understand virtualized clients
3.5 Understand application virtualization

## A Matter of Perspective

Regardless of the number of hours you may have logged as a computer user, you should approach this course with the eyes of an emerging technology professional. At the most basic level, an IT professional is expected to know how to set up (configure), update and maintain computer systems.

The specific job setting in which you may find yourself will often determine the method and approach you use. For example, manually configuring and updating one or two systems in a residential office is an easy task. Configuring and updating over a thousand machines across an enterprise network is a different story, and requires automated or semi-automated techniques, many of which may need to be deployed from a remote location.

To adequately prepare for the Microsoft Technology Associate Windows Operating System Fundamentals exam (98-349), you should:

- Understand the essential tasks required to configure, update and maintain the Windows 7 operating system.
- Understand the different challenges inherent in small residential networks, small-to-medium sized business networks, and enterprise-level networks.
- Be aware of the wide variety of tools and techniques that allow administrators in various job settings to perform essential tasks efficiently.

This course will present the essential tasks of operating system configuration and maintenance and provide hands-on experience in a localized setting. Enterprise-level and remote location deployments are beyond the scope of this course. However, you will also be introduced to various Web sites where you can find detailed information and explicit instructions on how to perform enterprise-level deployments.

# Reviewing the Basics

In this course, you will learn to install, configure and manage the Windows 7 operating system. Before delving into operating system specifics, it is important to review a few preliminary concepts pertaining to the function and operation of computer systems.

You should already be familiar with these concepts. If you require further information, see "Computer Basics" on the microsite.

Knowing where to locate information/instructions for performing specific tasks is one of the best tools an IT professional can possess.

## Hardware, Drivers, OS and Apps

A computer is a system that consists of various hardware components, various device drivers, an operating system, and any installed application software. Each of these "pieces" must interact with the others to provide a system that is functional and productive.

Hardware will be discussed momentarily. An *operating system* is a software program that controls all hardware and application software on the computer. *Device drivers* are small programs that enable the operating systems to communicate with the installed devices. *Application software* is used to perform certain functions such as word processing or database functions. Applications, also called programs, are installed on a computer system and must interact with the operating system in order to function.

## Hardware Essentials

Most modern computer systems are comprised of a system board and chip set, a central processing unit (CPU), one or more hard drives, an optical drive and system memory (RAM).

### Central Processing Unit (CPU)

The CPU is a silicon chip that processes instructions, manipulates data and controls the interactions of other circuits and components within the computer. Often, the term processor is used to refer to the CPU. A processor includes one or more cores. The core processes instructions and data. A dual-core process has two cores; a quad-core processor has four cores. Multi-core processors are common today. All the cores in a multi-core processor are combined onto a single silicon chip.

Do not confuse multi-core processors with systems that contain multiple processors (CPUs). Commercial servers, and high-end workstations and PCs may contain more than one physical CPU.

Processor speed is measured in units called hertz (Hz). The hertz (Hz) is the unit of frequency or cycles per second and is usually represented with the prefixes shown in the following table.

| Name | Abbreviation | Multiplies by | Equal to |
|---|---|---|---|
| Hertz | Hz | | 1 cycle per second |
| Kilohertz | KHz | One thousand | 1,000 cycles per second |
| Megahertz | MHz | One million | 1,000,000 cycles per second |
| Gigahertz | GHz | One billion | 1,000,000,000 cycles per second |
| Terahertz | THz | One trillion | 1,000,000,000,000 cycles per second |

A computer with a processor speed (or clock rate) of 500 MHz is running at 500,000,000 cycles per second. A computer with a clock rate of 2.8 GHz is running at 2,800,000,000 cycles per second. CPUs need 1 to 4 cycles to execute each instruction in a program, depending on the complexity of that instruction. Therefore, the general rule of thumb is that computers with higher processor speeds will execute more instructions in the same time period than those with slower speeds. This is a very simplistic view of how computer processing power is measured – computer manufacturers and technology enthusiasts often have lively debates over the complex aspects of this topic, which is beyond the scope of this course.

Operating systems and applications require a minimum processor speed to run successfully.

### 32-bit and 64-bit Processors

The basic structural design of a processor is called its architecture. A chip's architecture determines how much memory it can address and control, thereby also determining its performance speed. Processor architecture has evolved over time, offering increasing power and speed with each newer iteration. In the 1980s, most desktop systems used 16-bit processors. (Some of the most common 16-bit processors were the Intel 8086 and 80286 chips.)

By the mid-80s and early 90s, however, the 32-bit processor was common. Because the instruction set for a 32-bit processor is based on an expansion of the original 8086 chip instruction set, the term *x86* is commonly used to refer to the 32-bit class of processors. The 32-bit processor can address up to 4 GB of system memory (although applications are generally limited to 3.0 or 3.5 GB with the rest reserved for use by the operating system), and has found its way into servers, desktop systems and laptops all over the world.

Today, 64-bit processors are widely available. The term *x64* is used to refer to the 64-bit class of processors. A 64-bit processor can theoretically support up to 256 TB of physical system memory. However, system boards limit the amount of physical memory that can be installed, and operating systems often impose limits on how much physical memory can be addressed.

*Device drivers, operating systems and application software are written to conform to specific chip architectures – that is, they are designed to take advantage of the addressable memory made available.*

## System Memory

Memory, specifically system random access memory (RAM) is the main memory of a computer. It stores data and programs currently in use. RAM can store large amounts of information, but exists only when power to the computer is turned on. Once you power off the machine, you lose any information stored in RAM.

Physically, memory consists of chips mounted on small circuit boards that plug into memory banks on the system board. The more RAM a system contains, the faster its programs run. Considerable amounts of RAM are required for graphics, media playback and online gaming.

Having sufficient RAM in a system is essential for good performance. In many cases, sluggish performance is the result of too little RAM rather than inadequate processing power. Operating systems and applications require a minimum amount of RAM to run as designed. If your system has less than the recommended minimum requirement, the program may not run, or may perform poorly.

RAM capacity is typically measured in megabytes (MB) and gigabytes (GB). The following table lists standard capacity measurements:

| Measurement | Abbreviation | Equal to (approximately)… | About the same as… |
|---|---|---|---|
| bit | | A single binary digit | |
| byte | | Eight bits | One character |
| kilobyte | KB | 1,024 bytes (a "thousand" bytes) | Half a typewritten page |
| megabyte | MB | 1,024 KB (a "million" bytes) | One 500-page novel |
| gigabyte | GB | 1,024 MB (a "billion" bytes) | One thousand 500-page novels |
| terabyte | TB | 1,024 GB (a "trillion" bytes) | One million 500-page novels |

## Hard Drives and Optical Drives

Hard drives and optical media provide permanent storage space (that is, storage that persists whether the computer is on or off). Most computers contain at least one hard drive (some contain more than one physical hard drive). An operating system is installed on (that is, written to) the hard drive. When planning to install an operating system, it is important to ensure that there is sufficient hard drive space.

Optical drives read data from Compact Disc (CD), Digital Video Disc (DVD) or Blue-Ray (BD) media. Unlike hard drives, these discs can be removed from the optical drive and stored elsewhere. As a result, they are often used as backup media where valuable data can be stored in a safe location in case of a disaster. Operating systems are generally installed from CD or DVD, although they can be installed from other media, as you will learn later in this lesson.

Storage capacity for hard drives is measured in MB, GB or TB. Storage capacity for optical media is generally measured in MB and GB.

# Operating System Essentials

An operating system stores files, enables you to use software programs and (in tandem with device drivers) coordinates the use of computer hardware, such as the keyboard, mouse and printer. It also controls the computer's interaction and communication with the user.

Modern operating systems provide a graphical user interface (GUI), which enables a user to use a pointing device to point to objects, select options and functions, execute commands and launch application programs. (You will explore the GUI in the next lesson.) Application vendors design their programs to work within the environment provided by the operating system.

## APIs and Graphics Drivers

One of the ways in which application software interacts with Windows is through application programming interfaces, or APIs. An API is a complete set of all operating system functions that an application can use to perform tasks such as managing files and displaying information. The API also defines functions to support windows, icons, drop-down menus and other components of the GUI.

The graphics card in a computer system handles the graphics processing – it draws the screens and windows with which users interact. A graphics card is a circuit board that includes its own on-board memory, called graphics RAM or video RAM. Additionally, graphics cards support particular APIs and use specific device drivers.

Microsoft DirectX is a collection of APIs for handling multimedia tasks, especially game programming and video. Windows Display Driver Model (WDDM) is a device driver for graphics cards on systems running Windows Vista or higher.

Windows 7 requires a graphics card that supports DirectX 9, and uses a WDDM driver. As you will learn shortly, you can use the Windows 7 Upgrade Advisor to scan your system and determine if your video card is compatible. You can also use the Windows 7 Compatibility Center to find compatible hardware from various manufacturers.

## User Accounts

A Windows user account is a collection of information that controls what files and folders a particular user can access, and what changes that user can make to the system. Several users can share one physical computer through distinct user accounts. Each account is accessed through a user name and (optional) password.

The Windows 7 operating system provides three types of user accounts. These are:

| | |
|---|---|
| **Standard** | A standard user account is sufficient for normal computing. A standard user can generally run application programs, print, and use the Internet. However, a standard user cannot install or uninstall software, or make changes that affect other user accounts on the system. |
| **Administrator** | An administrator account is a user account that allows the user to make changes to the system that will affect other users. Administrators can change security settings, install and uninstall software and hardware, and access all files on the system. When Windows 7 is installed on a system, it automatically creates an administrator account to enable the installation and configuration of programs. The administrator account can then be used to create other user accounts. |
| **Guest** | A guest account is also automatically created when Windows 7 is first installed, but it is turned off by default. The guest account is provided for users who do not have a permanent account on the computer, but allows them to use the computer without providing access to the personal files of standard or administrator accounts on the system. Guest accounts provide access to a printer or to the Internet, for example. |

## Clients and Servers

A majority of computer users log onto systems that are part of a network. A *network* is simply a group of two or more computers connected in such a way that they can communicate, share resources and exchange data with one another.

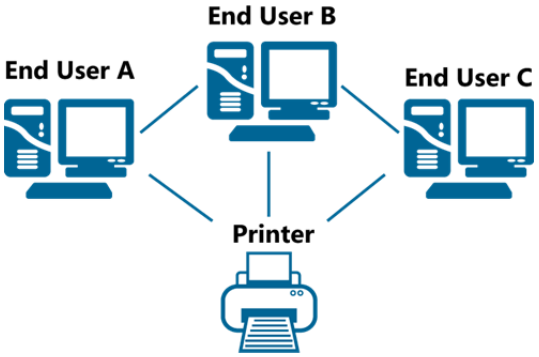
The terms client and server become important when discussing networking. A *client* is a system that requests a service or information from another computer on the network. Any PC connected to a network is considered a client – it requests Internet access or print services from another computer on the network. Client systems run a client operating system, and are intended to be used directly by users. When a user is finished for the day, he or she is free to turn off the system without affecting anyone else. Windows XP, Vista and Windows 7 are all examples of client operating systems.

A *server* is a computer in the network that manages network resources and/or provides information and services to clients on the network. For example, servers are used to run security software that determine who can access the network, and run routing software that directs which programs and services a particular client system can use. Servers run a specialized server operating system, and are generally more powerful than client systems. For this reason, server operating systems support the use of multiple processors and some support server clustering (which is the process of combining the computing power of several servers in order to achieve super-computing speeds). Servers are expected to remain up and running at all times; in fact, server operating systems require that you enter a reason for powering the system off. Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 are examples of server operating systems.

Windows 7 and Windows Server 2008 R2 are client and server operating systems based on the same code. These two operating systems are used together in corporate networks.

### Peer-to-peer Networks

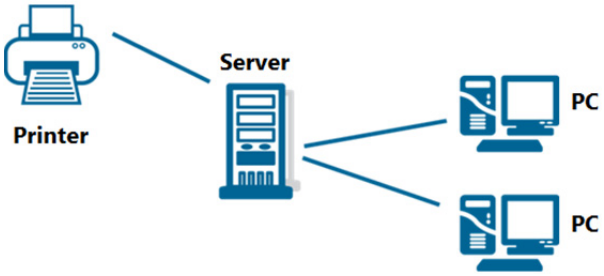
Most home and small office networks consist entirely of client systems. These types of network are called peer-to-peer networks. A *peer-to-peer network* is one in which all the participating computers are more or less equal, and there is no central server or centralized management of network resources. Each computer connected to a peer-to-peer network is called a host, and hosts act as both clients and servers. When a host is sharing a resource (such as a file, a printer), it is acting as a server. When a host requests a service or information from another host, it is acting as a client. The following figure illustrates a peer-to-peer network:




Any computer on a peer-to-peer network can communicate with any other computer on the network. A Windows 7 HomeGroup (or in previous versions of the Windows operating system, a Microsoft Windows Workgroup) is an example of a peer-to-peer network.

### Server-based Networks

In most business settings, networks are server-based. A server-based network is one in which one or more servers centrally manage the network and control access to its resources. Individual computers and networking devices on a server-based network are referred to as nodes. Nodes interact with one another through one or more servers to which they are all connected. A server-based network is shown in the following figure:




## Domains, Workgroups and HomeGroups

Domains, workgroups and HomeGroups represent different methods for organizing and managing computers and other resources on a network.

Computers running Windows on a network must be part of either a workgroup or a domain. Computers running Windows on home networks can also be part of a HomeGroup, but that is not required.

### Workgroups

A workgroup is a named group of computers on a peer-to-peer network. The default workgroup name in Windows 7 is: WORKGROUP. Additionally,

- All the computers in a workgroup are peers.
- Each computer in the workgroup has its own set of user accounts. In order to access a particular computer in the workgroup, you must have an account on that computer.
- All computers in the workgroup must be on the same local network.
- A workgroup is not protected by a password.

Theoretically, workgroups support up to 20 computers. However, in practical application, 10 systems is about the most that can be well-supported.

### HomeGroups

Computers on a home network must belong to a workgroup, but they can also belong to a HomeGroup. Computers in a HomeGroup:

- Must explicitly join the HomeGroup by supplying the HomeGroup name and password.
- Can easily share pictures, music, video, documents and printers with other computers in the HomeGroup without requiring an account on each computer in the HomeGroup.

You will learn more about HomeGroups later in the course.

Home Groups are not supported in Windows Server 2008 R2.

### Domains

Most corporate networks today are domain-based or directory-based networks. A domain is a logical collection of network resources. The domain is centrally managed by a server designated as the domain controller. In a domain, there is one master list of users and their corresponding privileges. Domain services were first introduced in Windows NT networks.

Large-scale network management today is usually handled through directory-based networking or directory services. In a directory-based network, all network resources (servers, workstations, printers, users, files, etc.) are treated as objects. Network objects are stored in a hierarchical directory. This directory is copied to directory servers throughout the network.

In Windows networks, directory services are implemented through Active Directory. A (directory) server running Active Directory is called a domain controller.

Active Directory was first released with Windows 2000 server, and has been revised and improved through successive server operating systems. In Windows Server 2008 R2, the domain controller role was renamed Active Directory Domain Services.

The following are important points to remember about domains:

- One or more computers are servers. The servers manage and control the domain and all its resources.
- Domain users must specifically log on to the domain by supplying a user name and password.
- A domain user can log on to a domain from any computer connected to the network, regardless of whether the user has a user account on that specific machine.
- The users in a domain can be on different local networks.
- Domains can support thousands of computers.

## Licensing and Activation

When you purchase operating system software, you are purchasing a license, or the right to use the software on a computer. Windows 7 can be purchased for use on one or more systems, depending on the terms of the license agreement.

Additionally, after you install Windows 7 you must activate the product before you can use it. Product activation is a license validation procedure that requires you to enter a valid product key. The Windows product key is typically located on an orange or yellow sticker on the back of a CD case or DVD case. The product key is a string of 25 characters, divided into groups of 5 characters each.

There are three basic types of licensing options for Windows 7:

| | |
|---|---|
| **Retail** | You purchase the software from a retailer and bring it home in a box that includes a manual, holographic discs and a license. A retail product can be activated as many times as necessary as long as it is not installed on more computers than the license allows at the same time. The first activation can typically be performed online, while subsequent activations require that you use the telephone activation service, as you must confirm that you are not activating the product on a second PC without having removed it from the first one. |
| **Original Equipment Manufacturer (OEM)** | The software comes preinstalled on a new PC. OEM licenses are meant to be used only on the PC with which they were originally supplied, and can be activated only on that original PC. |
| **Volume Licensing** | Available to organizations that require five or more licenses. One product key is used for all the installations and the software is usually supplied as a download or on Volume Licensing-branded discs. Activation for volume licenses can be performed through the use of either a Key Management Service (KMS) or a Multiple Activation Key (MAK). A KMS runs on a server (called the KMS host) in an organization's local network. Individual systems connect to the KMS host for activation instead of using Microsoft's hosted activation service. A MAK includes a pre-determined number of allowed activations per the terms of the volume licensing agreement. Each time a system activates with Microsoft's hosted activation service, the number of remaining allowed activations is decremented. |

# Windows Operating System Versions and Editions

Objective 2.1 2.4

There are several versions and editions of the Windows operating system in current use around the world. As an IT professional, you should be aware of the versions and editions available and understand how to make a sound choice when selecting an operating system for your organization.

An operating system *version* refers to the specific code base that was used to develop the operating systems. Currently, the most common versions of Windows client operating systems running on systems around the world are: Windows XP, Windows Vista, and Windows 7.

Each version of Windows comes in different editions. The operating system *edition* determines which features are available. Generally, the lower the edition, the fewer the features. That is, a basic edition has fewer features than a premium edition or a professional edition.

Additionally, each version and edition of Windows (with the exception of Windows 7 Starter) comes in a 32-bit and a 64-bit version.

The available Windows 7 editions are described in the following table. Of the six editions, only Home Premium, Professional and Ultimate are widely available for retail purchase.

| | |
|---|---|
| **Windows 7 Starter** | Starter only comes preinstalled on new systems with low-end processors – such as netbooks, which are designed primarily for accessing the Internet. Starter is not available for retail sale; that is, you cannot purchase a copy of Windows 7 Starter. The Windows Aero theme is not included, and the Desktop wallpaper and visual styles are not user-changeable. Starter supports a maximum of one physical CPU (although each CPU can have multiple cores), comes in a 32-bit version only, and can address up to 2 GB of RAM. Starter is designed to perform basic computing tasks, such as accessing the Internet, sending e-mail and creating documents. Most of the advanced Windows 7 features are not supported. |
| **Windows 7 Home Basic** | The Home Basic edition is available in emerging markets (e.g., China or India) only, where it can be purchased preinstalled or through a retail supplier. Home Basic supports a maximum of one physical single or multi-core CPU. The 32-bit version can address up to 4 GB of RAM. The 64-bit version can address up to 8 GB of RAM. Home Basic includes only partial support for the Aero interface. |

| | |
|---|---|
| **Windows 7 Home Premium** | Home Premium is the lowest edition available for purchase in retail stores in existing markets. (It is also available as an OEM license.) Home Premium supports a maximum of one physical single or multi-core CPU. The 32-bit version can address up to 4 GB of RAM. The 64-bit version can address up to 16 GB of RAM. The full Aero interface is supported in Home Premium. |
| **Windows 7 Professional** | Professional includes all the features of Home Premium and is the lowest edition that provides the ability to join a domain and the ability to operate as a remote desktop server. It is also the lowest edition that supports two physical single or multi-core CPUs, supports backing up to a network location, and supports Windows XP mode. (You will learn about XP mode later in this lesson.) Professional can be purchased OEM, retail or with volume licensing. The 32-bit version can address up to 4 GB of RAM. The 64-bit version can address up to 192 GB of RAM. |
| **Windows 7 Ultimate** | Ultimate edition is available to anyone as an OEM or retail license. Ultimate includes all the features of Professional and adds enhanced features such as BitLocker and AppLocker (you will learn about these features later in the course) and support for Multilingual User Interface (MUI) packages, UNIX applications and booting from a virtual hard disk. Ultimate supports a maximum of two physical single or multi-core CPUs. The 32-bit version can address up to 4 GB of RAM. The 64-bit version can address up to 192 GB of RAM. |
| **Windows 7 Enterprise** | Enterprise edition is available only to volume licensing customers. It is essentially the same as Windows 7 Ultimate, except that it is not available as an OEM or retail license. |

## Sub-editions

Sub-editions are editions of the operating system designed for sale in specific markets. The release of sub-editions was a response to legal pressures in certain countries regarding user freedom of choice in selecting and installing media player, instant messaging and Internet browser software. There is no difference in cost between a "regular" edition and a sub-edition. For Windows 7, the following sub-editions are available:

- Windows 7 N (Starter, Home Premium, Professional, Ultimate and Enterprise) – designed for the European market. This sub-edition includes the same functionality as Windows 7 but does not include Windows Media Player 12 and related programs, such as Windows Media Center or Windows DVD Maker. Users must install their own media player and software to manage and play CDs, DVDs and other digital media. If the user wishes to install Windows Media Player 12 and its related technologies, the software is available as a free download.
- Windows 7 E – also designed for the European market, including the UK. This sub-edition includes the same functionality as Windows 7 but does not include Internet Explorer 8 (IE8).
- Windows 7 K – designed for the Korean market. This sub-edition includes the same functionality as Windows 7 and includes links to a Media Player Center Web site and a Messenger Center Web site which allow users to download third party media players or instant messaging software.
- Windows 7 KN – also designed for the Korean market. This sub-edition includes the same functionality as Windows 7 K but does not include Windows Media Player and its related technologies, does not include links to download Windows Live Messenger or links to any third party Media Player or Messenger Center Web sites.

## Comparing Edition Features

While having a broad idea of what each edition offers is a good starting point, it is important for an IT professional to compare the features offered in each edition in order to make an informed recommendation/choice for selecting an operating system for the organization. The following table compares the editions based on several features employed in various sized businesses.

| Feature | Home Premium | Professional | Ultimate/Enterprise |
|---|---|---|---|
| Join a HomeGroup | Yes | Yes | Yes |
| Join a Domain | No | Yes | Yes |
| Support for XP Mode | No | Yes | Yes |
| Remote Desktop server | No | Yes | Yes |
| Network Backup | No | Yes | Yes |
| Group Policy Controls | No | Yes | Yes |
| Encrypting File System | No | Yes | Yes |
| AppLocker | No | No | Yes |
| BitLocker | No | No | Yes |
| BranchCache | No | No | Yes |
| DirectAccess | No | No | Yes |

The features listed in the table are briefly described below. You will learn about these features in more detail throughout the course.

| | |
|---|---|
| **XP Mode** | Provides compatibility for older programs by running those applications in Windows XP through the use of virtualization software. |
| **Remote Desktop server** | Allows other computers to connect to this computer using the Remote Desktop Connection feature. |
| **Network Backup** | Allows you to backup files to a network location. |
| **Group Policy Controls** | Allows network administrators to control users and computers within the network. For example, an administrator can define a user's work environment one time, and then group policy continually enforces those settings. Group policy applies to domain-based networks. |
| **Encrypting File System (EFS)** | Allows you to store particular information on a hard disk (e.g., files or folders) in an encrypted format. |
| **AppLocker** | Allows network administrators to control which applications users can run and helps control the use of unauthorized software on corporate systems. |
| **BitLocker** | Enables automatic encryption of internal drives and removable media. |
| **BranchCache** | Enables content from servers outside the local area network to be cached (that is, stored) on local computers (computers within the local area network) for fast access. BranchCache improves application response time and reduces the amount of traffic flowing into and out of the local network. |
| **DirectAccess** | Allows remote users to securely access network resources without having to connect through a virtual private network (VPN). DirectAccess establishes a connection between a corporate network and a user's portable computer every time that computer accesses the Internet. This allows the user to seamlessly access the network, and allows network administrators to manage the remote systems even when they are not connected to the VPN. |

# Understanding 32-bit and 64-bit Operating Systems

Each Windows 7 edition (with the exception of Starter) is available in a 32-bit version and a 64-bit version. There are advantages and disadvantages to each.

### 32-bit Operating System

The 32-bit version of Windows will run on a system with either a 32-bit processor or a 64-bit processor.

This version can run 32-bit applications and most 16-bit applications. While most modern software is designed to run on 64-bit machines, many companies have significant money invested in old applications, or custom-built applications that were created to run on older hardware.

A 32-bit operating system can address only up to 3.5 GB of RAM (or less), regardless of how much physical RAM is installed on the system.

### 64-bit Operating System

The 64-bit version of Windows will run on a system that has a 64-bit processor. It will not run on a system with a 32-bit processor.

This version can address up to 8 GB of RAM in the Home Premium version, and up to 192 GB of RAM in the Professional and Ultimate/Enterprise version.

This version can run 64-bit applications and most 32-bit applications. However, some 32-bit applications include 16-bit artifacts. Artifacts are old portions of code or sub-routines found within an application. If a 32-bit application includes 16-bit artifacts, the application will not run or will not perform well on a 64-bit operating system. (As you will learn shortly, Windows XP mode can provide a solution for running these older applications.)

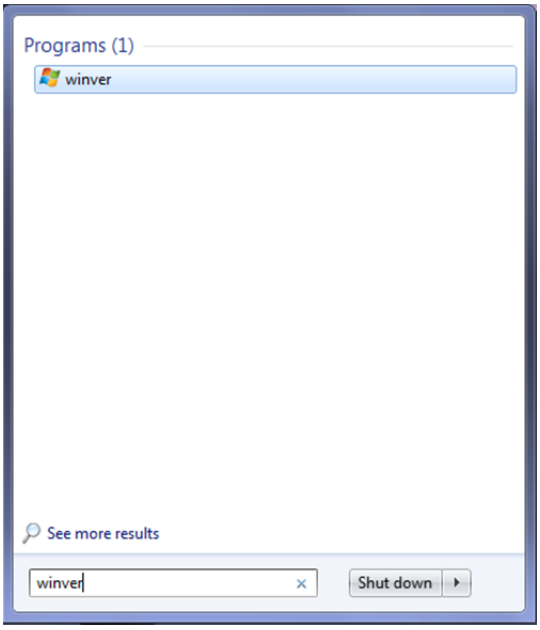
If you elect to run a 64-bit version of Windows 7, you must be sure that you can obtain and install 64-bit device drivers for your devices (e.g., scanners and printers). The 64-bit version of the operating system is not compatible with 32-bit drivers.

To check whether a device includes 64-bit drivers you can check the product documentation, visit the manufacturer Web site, or visit the Windows 7 Compatibility Web site at www.microsoft.com/windows/compatibility/windows-7.

## Exercise 1-1: Determining Your Operating System Edition

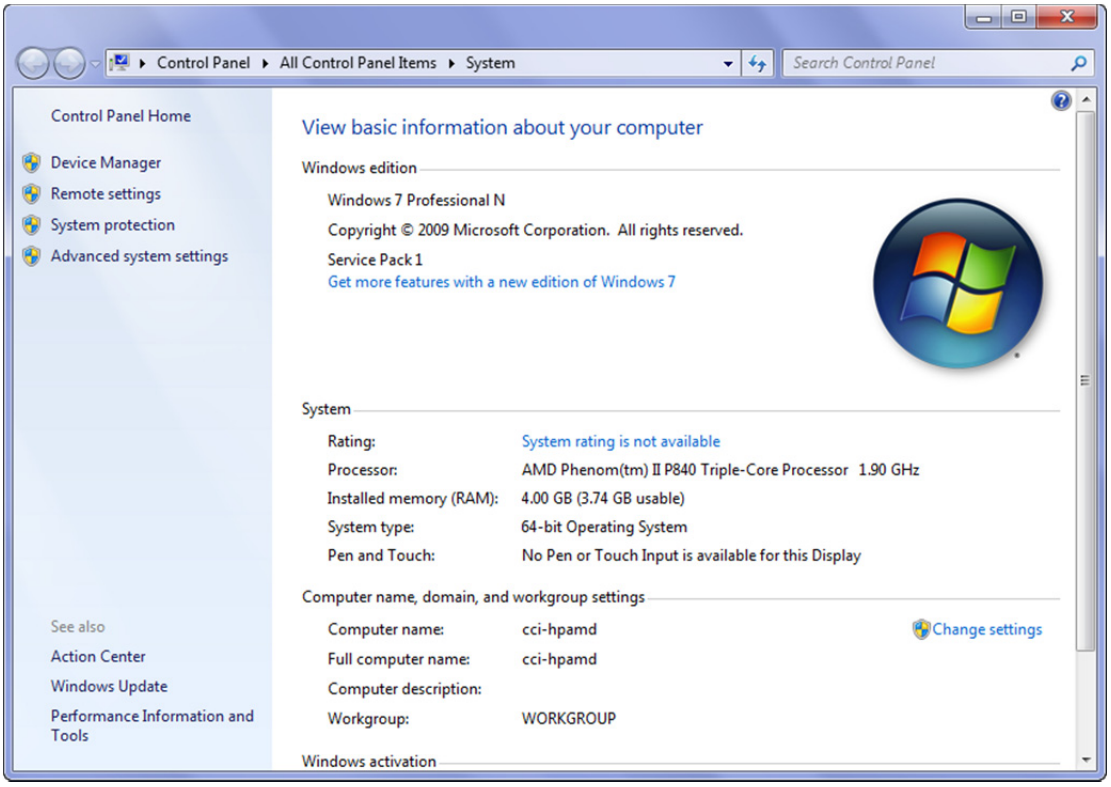

In this exercise, you will determine which edition and bit-level of Windows 7 you are running.

1. Click the **Start** button, then in the search box that displays at the bottom of the search menu, type: `winver`.




2. The Start menu displays the winver program at the top of the list. Click **winver** to open an About Windows dialog box. Notice that the information indicates the edition, but not the bit level.


3. Click **OK** to close the About Windows dialog box, then click **Start**, right-click **Computer**, then click **Properties** to open the System page of the Control Panel. The edition and bit level are indicated on this screen.




4. Close the Control Panel window.

In this exercise, you determined which edition of Windows 7 you are running.

# Understanding Windows Anytime Upgrade

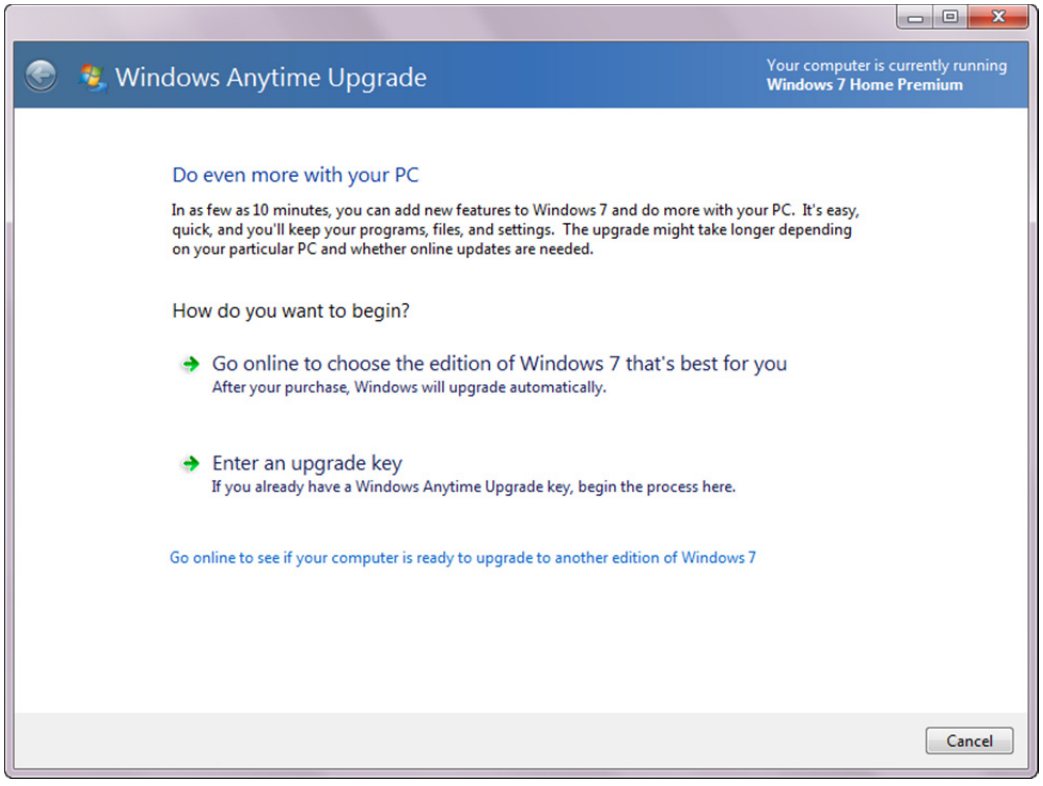
Instead of creating separate installation code for the different editions of Windows 7, Microsoft includes all the features of all editions in every installation pack. When a user purchases a Windows Anytime Upgrade, he or she is purchasing an upgrade key (a new software license) which activates the appropriate enhanced features. Upgrade keys can be purchased from retailers, or online from Microsoft.

Windows Anytime Upgrade is a feature built directly into the operating system. You can use Anytime Upgrade to upgrade from one edition of Windows to another within the following limitations:

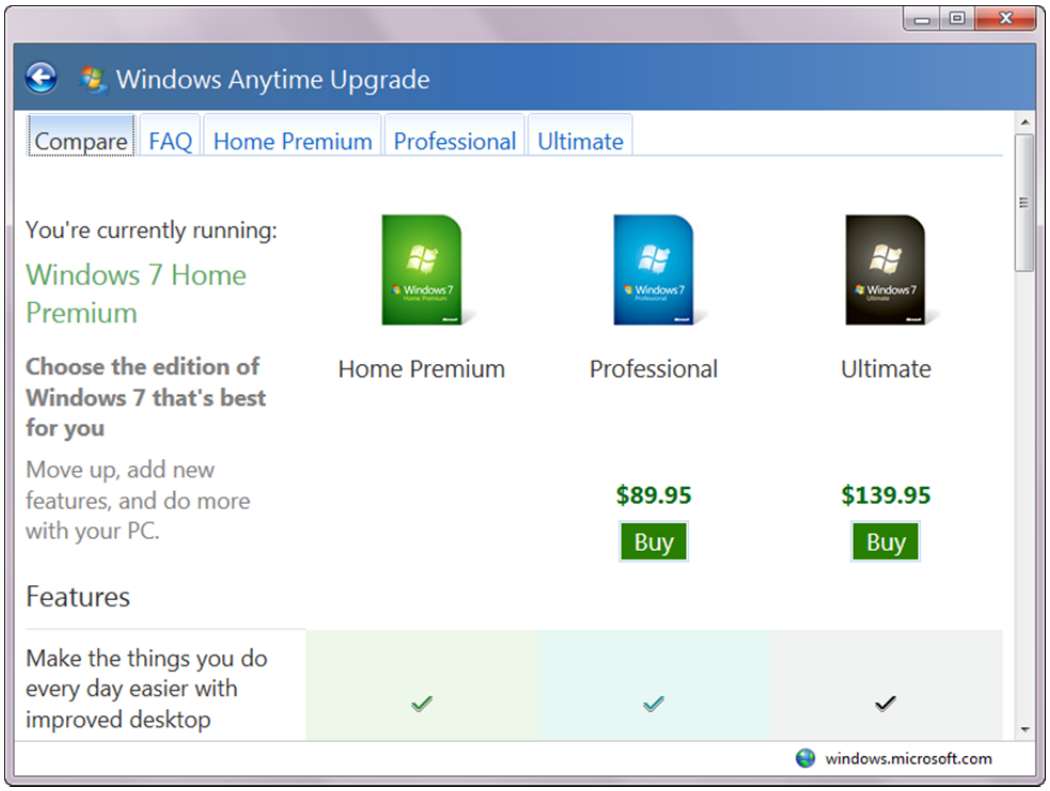
- You can upgrade to a higher-level edition, but you cannot downgrade. For example, you can upgrade from Professional to Ultimate, but you can't go from Professional to Home Premium.
- You can upgrade only within the same bit level. That is, you cannot upgrade from Home Premium 32-bit to Professional 64-bit.
- You cannot use Windows Anytime Upgrade to upgrade from a previous version of Windows. That is, you cannot use Anytime Upgrade to upgrade from Windows Vista to Windows 7.

To use Windows Anytime Upgrade, you must be running an activated copy of Windows. Because the purchase of an upgrade key simply makes the enhanced features available, you can upgrade your current edition of Windows 7 without having to perform an installation. This allows you to keep your programs, files and settings intact, and is the easiest way to upgrade to a new (same bit-level) edition.

You can launch Windows Anytime Upgrade from the Start menu. Click the **Start** button, click **All Programs**, then click **Windows Anytime Upgrade** to open the Windows Anytime Upgrade dialog box. You can enter an upgrade key or go online to select the edition of Windows 7 you want to purchase.




If you elect to go online, you are presented with the available upgrades.




When you click the **Buy** button, you are prompted to enter your purchase information and will be provided with an upgrade key.

# Planning for Windows 7 Installation

Objective 2.1

Any installation of Windows 7 should begin with proper planning. When you have identified the edition of Windows you think you want to use, you must ensure that your computer system(s) meet (or preferably, exceed) the minimum system requirements. You should also be sure to identify any compatibility issues and their solutions before installing.

## System Requirements

You must ensure that a system meets the minimum requirements before installing any application or operating system. The minimum requirements are determined by the software vendor.

The minimum system requirements to run Windows 7 Starter and Home Basic are:

- 1 GHz or faster x86 or x64 processor
- 512 MB RAM
- 16 GB hard disk space (Starter); 20 GB hard disk space (Home Basic) plus 15 GB free space
- DirectX 9 graphics card with WDDM 1.0 and at least 32 MB video RAM

The minimum system requirements to run Windows 7 Home Premium, Professional, Ultimate and Enterprise are:

- 1 GHz or faster x86 or x64 processor
- 1 GB RAM (32-bit); 2 GB RAM (64-bit)
- 40 GB hard disk space plus 15 GB free space
- DirectX 9 graphics card with WDDM 1.0 or higher and at least 128 MB video RAM

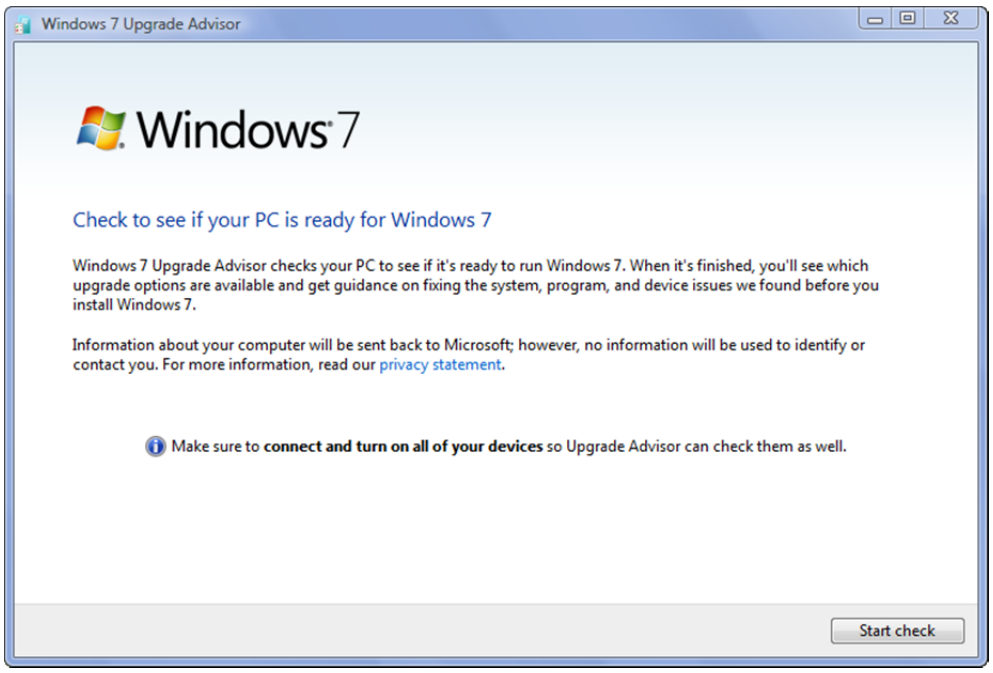
Keep in mind that minimum system requirements are the bare minimum required for the software to run. It is strongly recommended that a system exceed the minimum requirements to ensure that the software performs well. Most organizations establish a standard baseline for their systems to ensure uniform performance across the enterprise.

A common baseline for Windows 7 is:

- 2 GHz total processing power (includes multiple cores and/or multiple processors)
- 2 GB RAM
- DirectX 9 graphics card with WDDM 1.0 or higher with at least 512 MB video RAM
- 80 GB hard drive

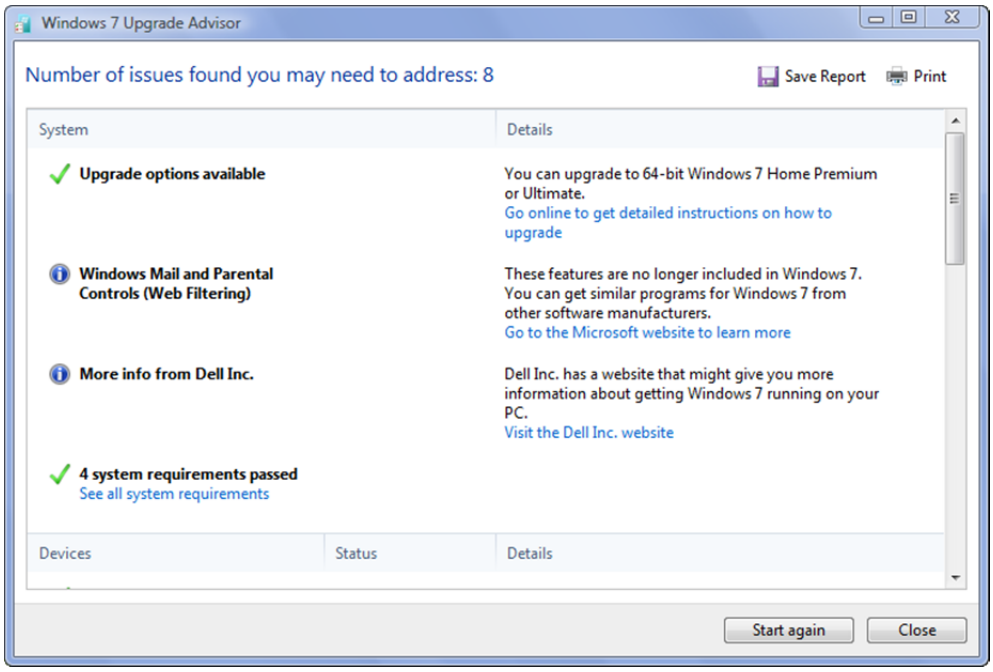
## Using the PC Upgrade Advisor

You can use the PC Upgrade Advisor (also called the Windows 7 Upgrade Advisor) to determine if a particular system is capable of running Windows 7 and to generate a report of any potential compatibility issues with installed programs and connected devices. It is supported on Windows 7, Windows Vista, and Windows XP Service Pack 2.

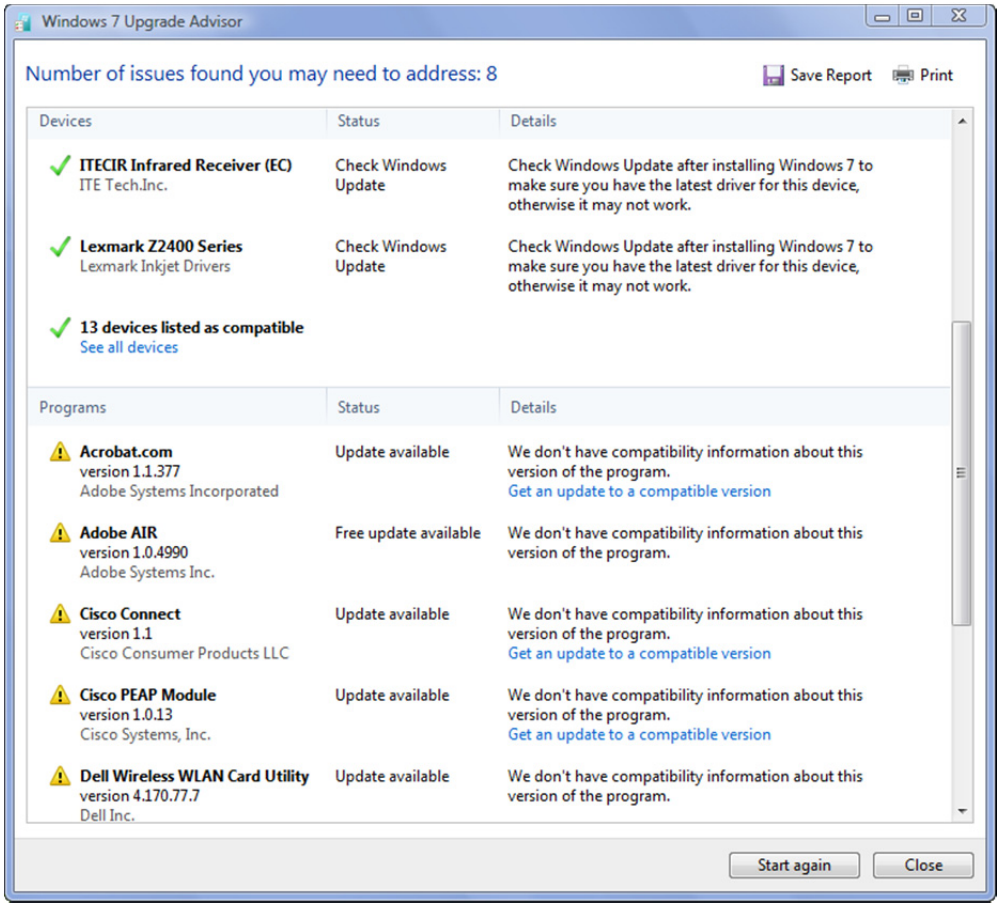



Upgrade Advisor can be used on a system running a previous version of Windows to determine whether the system will readily support Windows 7, or it can be used on a system currently running an edition of Windows 7 to determine if Anytime Upgrade can be used to upgrade to a higher edition. Upgrade Advisor checks the system and any connected devices (such as printers, cameras, scanners, etc.) and reports on system readiness to run Windows 7 and lists any potential compatibility issues with devices, device drivers and installed applications.

The results screen indicates which editions you can use and tells if your system meets the minimum hardware requirements. For example, the results screen in the following figure indicates that the system will support Windows 7 Home Premium or Ultimate. It also indicates that certain Windows Vista features, such as Windows Mail and Parental Controls, are not supported in Windows 7.




Upgrade Advisor will also list any device drivers or application programs that may have compatibility issues with Windows 7. Where possible, Upgrade Advisor provides links for finding compatible program versions, compatible hardware drivers, etc.



You need to download and install PC Upgrade Advisor from the Microsoft Web site. Once installed, it can be launched from the Windows Start menu. Note that you must be logged on with an Administrator account, or provide an administrator user name and password in order to run Upgrade Advisor.

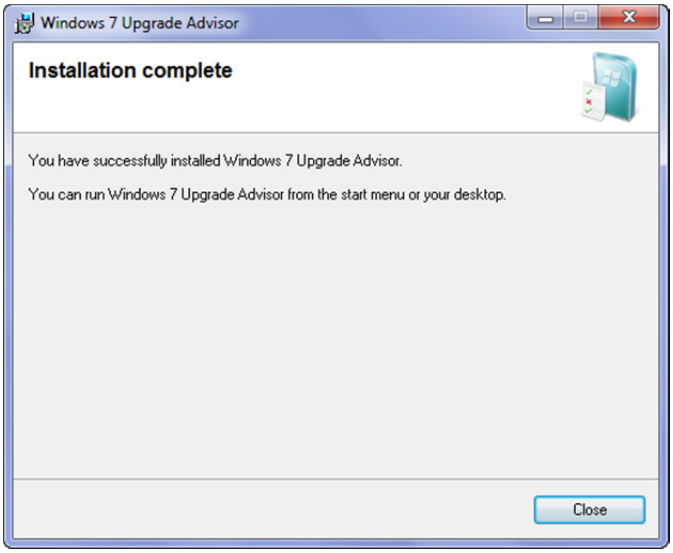
## Exercise 1-2: Using PC Upgrade Advisor

In this exercise, you will download, install and run the PC Upgrade Advisor.

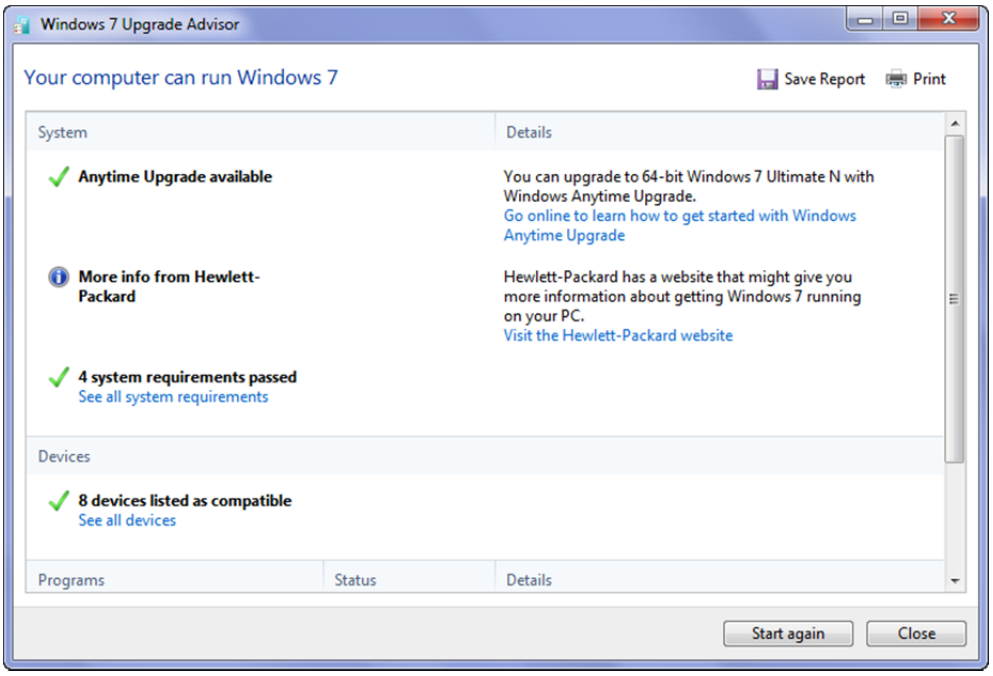
1. Open a Web browser and go to http://windows.microsoft.com/upgradeadvisor to view the Windows 7 Upgrade Advisor page.
2. Scroll to the bottom of the page and click the **Download the Windows 7 Upgrade Advisor** button to go to the Download Center page.
3. In the Quick details section, click the **Download** button. If you are presented with additional downloads, do not select any, then click the **Next** button.
4. When prompted to Run, Save or Cancel the download, click **Run** to begin the download and installation.
5. When the User Account Control agent appears, click **Yes** to allow the program to make changes to the computer and launch the setup wizard.

**Note:** Throughout this lesson and all subsequent lessons, when the User Account Control agent appears, click **Yes** unless directed otherwise.

6. Select **I accept the license terms**, then click the **Install** button to begin the installation. When the installation is complete, click the **Close** button.




7. Close the Web browser. You can now run the upgrade advisor from the Start menu.
8. Click **Start**, click **All Programs**, then click **Windows 7 Upgrade Advisor** to start the program.
9. As advised in the first screen, be sure to connect and turn on all devices so that the upgrade advisor can check them, then click the **Start check** button to proceed. It may take several minutes for the upgrade advisor to run. At completion, a results screen similar to the one shown below will display.

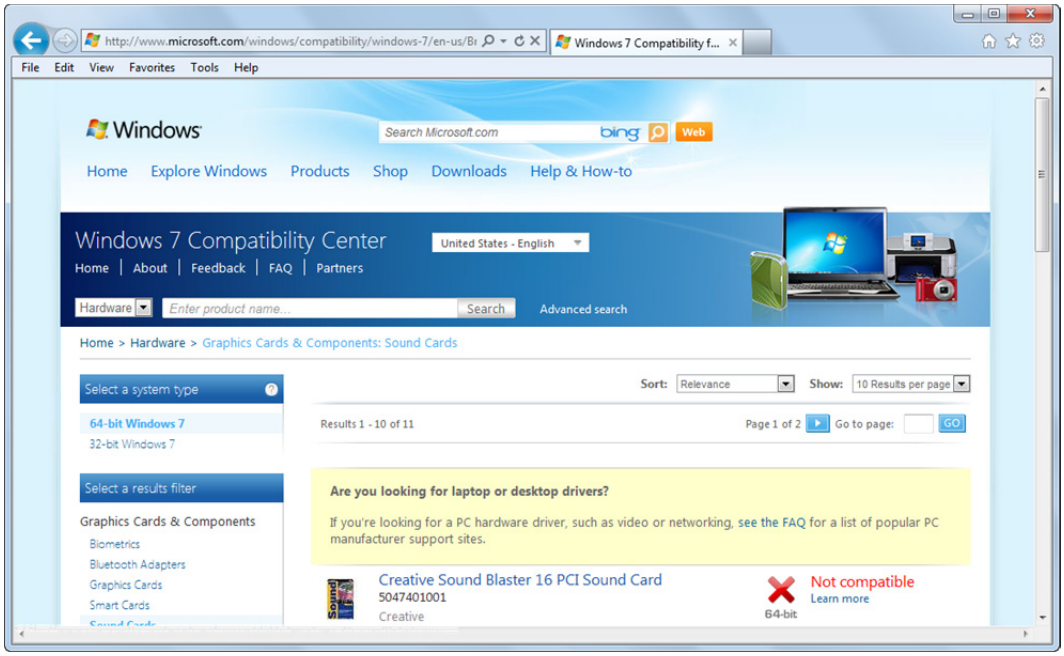



10. Which higher editions (if any) of Windows 7 will your system support?
11. Scroll through the results. Are all your devices compatible? Are all your programs compatible?
12. When you are finished reviewing your results, click the **Close** button.

In this exercise, you used the PC Upgrade Advisor.

## Windows Compatibility Center

You can also use the Microsoft Windows 7 Compatibility Center Web site to check the compatibility of hardware and software. It is useful if you are not able to use the PC Upgrade Advisor; e.g. you are currently using a different computer than the one that will be upgraded. The Compatibility Center lists thousands of popular devices and applications (for both 32-bit and 64-bit systems).



By searching for a particular product, you can easily determine whether it will work with Windows 7, if an upgrade might be required, or if there is no compatible version available.


You can use the site to download device drivers and software updates. The site also provides links to manufacturer Web sites.

## Exercise 1-3: Using the Compatibility Center


In this exercise, you will explore various features of the Windows 7 Compatibility Center Web site.

1. Open a Web browser and visit www.microsoft.com/windows/compatibility/windows-7.
2. Click in the **Enter product name** text box, type: `Office 2000` then click the **Search** button. Notice that you must pay for an upgrade to find a version that will work on a 64-bit operating system.
3. In the navigation bar near the top of the window, click the **Home** link to return to the Compatibility Center home page.
4. Hover the mouse pointer over the **Security** icon, then click **Anti-spyware** in the shortcut menu to view a list of anti-spyware applications.
5. In the navigation pane at the left side of the page, scroll down to the **Compatibility** section, then under Compatibility, click **Not compatible** to view only anti-spyware applications that are not compatible with Windows 7.
6. Return to the Compatibility Center home page, then click the **Hardware** tab.
7. Click in the **Enter product name** text box, type: HP `Scanjet` then click the **Search** button. Are all the HP scanners compatible?
8. For any product on the page, click the **Learn More** link. What type of information is available?
9. How easy or difficult do you think it would be to find out if a product you own is compatible with Windows 7?
10. If you were planning to upgrade an organization's computers, how would you use the Compatibility Center?

In this exercise, you explored the Windows 7 Compatibility Center Web site.

# Windows 7 Upgrade Versus Clean Install

Windows Easy Transfer is supported in Windows XP, Windows Vista and Windows 7.

Objective 2.2

When you have decided which edition of Windows 7 to install, the next step is determining whether to perform an upgrade or a clean install.

## Upgrade

When you perform an *upgrade*, existing user settings, files and installed applications are retained and you do not need to reinstall them. When you boot from the Windows 7 installation DVD, the default option is to perform an upgrade.

A true in-place upgrade to Windows 7 is supported only from Windows Vista Service Pack 1, and this upgrade must maintain the same bit level. To upgrade from a version of Windows prior to Windows Vista Service Pack 1, you would first have to upgrade to Vista SP1 and then upgrade from there to Windows 7.

Even when moving from Windows Vista SP1 to Windows 7, you have the option of performing a clean install instead of an upgrade.

# Clean Install

When you perform a *clean install*, you should re-format the hard drive before installing Windows 7. Thus, the operating system files are installed fresh, user settings must be configured anew, user files and any programs that were installed on the system prior to the clean install must be reinstalled and reconfigured. Any user documents that need to be retained must be copied to back up media before the clean install, and then copied back onto the system after the new operating system installation is complete.

You must perform a clean install if you want to change the bit-level of the operating system or if you want to move from a version of Windows prior to Windows Vista SP1 to Windows 7.

Because all existing settings, files and applications are destroyed when you perform a clean install, you must take steps to migrate your files, folders and settings (if you want to retain them) to the new installation. This process involves copying the data you want to retain to backup media and then transferring it to Windows 7 after the clean install has been performed.

Windows Easy Transfer is a tool designed to facilitate the transfer of data and settings from one operating system to another, and will work for transferring data between operating systems on the same computer or on different computers. You can use Windows Easy Transfer to migrate settings, user accounts files, music, pictures, e-mail, videos, and Internet favorites.

Additionally, you must ensure that you have access to the installation discs for any applications you want to reinstall on the new Windows 7 system. Windows Easy Transfer cannot migrate applications. You should also have access to any required device drivers if they are not available through Windows.

Of course, you can also perform a clean install and elect to discard all previous settings and files.

# Identifying Upgrade Paths

Objective 2.2

As an IT professional, you should understand the available paths for upgrading from various operating systems to Windows 7.

## From Windows XP

To upgrade from Windows XP you can:

- Upgrade first to Windows Vista SP1, then upgrade to Windows 7,
- Perform a clean install directly to Windows 7 and migrate all existing application program settings using Windows Easy Transfer, or
- Perform a clean install directly to Windows 7 and discard the old settings.

## From Windows Vista

To upgrade from Windows Vista you can:

- Apply Service Pack 1 and then upgrade to Windows 7,
- Perform a clean install of Windows 7 and migrate the existing application program settings using Windows Easy Transfer, or
- Perform a clean install of Windows 7 and discard the old settings.

## From Earlier Versions of Windows

To upgrade from earlier versions of Windows such as Windows 95/98/ME or 2000 you can:

- Upgrade through multiple Windows versions up through Windows Vista SP1, then upgrade to Windows 7, or
- Perform a clean install directly to Windows 7 and discard the old settings.

## From Non-Microsoft Operating Systems

To upgrade from a non-Microsoft operating system, you must:

- Perform a clean install.

If you want to retain your old data files, you can copy them to backup media and copy them back after Windows 7 has been installed. To open these old data files, however, you must find and install application software that is both compatible with Windows 7 and compatible with your old files.

## Application Compatibility

There are various reasons that applications stop functioning or perform erratically after an operating system upgrade. These reasons can include:

- Applications may include artifacts which use a bit level that is no longer supported.
- Applications may rely on features that were supported in previous versions of Windows but are no longer supported.
- Applications may be incompatible with new features in the upgraded operating system. For example, the Windows User Account Control feature is designed to allow users to perform their work tasks while logged on to the system as standard users. In previous versions of Windows, many users logged on as Administrators. Older applications may expect the user to have administrative rights on the system and certain application functions may crash because the user does not have sufficient rights or privileges.

### Identifying Issues

As you have seen, using the Upgrade Advisor and the Compatibility Center can alert the system administrator to potential application compatibility issues. These tools are well suited for a small computing environment. However, identifying potential issues across an enterprise can be a different story.

In large enterprises, thousands of machines may be running various versions of application software on hardware platforms of varying power. Microsoft provides the Application Compatibility Toolkit (ACT) for inventorying applications and identifying and possibly creating fixes for potential compatibility issues. The toolkit includes:

| | |
|---|---|
| **Application Compatibility Manager (ACM)** | Creates modules that can be distributed to client computers to inventory hardware and software and analyzes the collected information. |
| **Standard User Analyzer (SUA)** | This tool is used to locate specific items in the application that cause a failure so that these items can be corrected. The fixes that are discovered with this tool are collected into a shim. A shim is a collection of fixes that are intended to make an application work on Windows 7. Shims are stored in shim databases. |
| **Compatibility Administrator** | This tool is used to view and manage shim databases. |

### Remediating Issues

Some applications that won't work in Windows 7 can be made to work through the use of application shims. Other applications may need to be upgraded to a version that is compatible with Windows 7.

It may seem an obvious solution that if an application won't function in Windows 7, it should be updated to a newer compatible version or replaced with another software package that can perform the same tasks. In many cases, this can be the appropriate solution.

However, consider the cost of upgrading thousands of copies of a software package. Consider also that some applications are custom-built for an organization and that upgrades or replacements may not be available. For these situations, virtualization may offer the best solution. (You will learn about virtualization shortly.)

# Deployment Options

Objective 2.3

Upgrading one or two PCs in a home or very small business make take an hour or two. However, as you increase the number of systems to be upgraded, the time required to sit at each one and perform a manual installation adds up quickly. In large enterprises, the number of systems that require updating may be truly staggering, which makes it highly impractical for even a large IT staff to perform all the installations "live and in-person."

For this reason, various tools and methods are available for installing Windows 7. Some are suited for home users and small businesses, while others are geared for large enterprises which support a substantial infrastructure. These installation methods and deployment strategies are discussed in the following sections.

# Preliminary Concepts

Before examining installation methods, you should understand the following concepts about how computers locate and load operating system software.

| | |
|---|---|
| **Boot disk** | A removable medium from which a computer can load and run an operating system or utility program. The process of loading such a program is called "booting." Boot disks are used for several purposes, including data recovery, hardware and software troubleshooting, and operating system installation. A boot disk must be created in a specific manner so that it is bootable – that is, you cannot simply copy operating system files to a DVD or flash drive and use it to boot a system. You must take specific steps to make the media bootable. |
| **Boot sequence** | Most computers boot (load the operating system) from the hard drive. However, a computer can also load an operating system from a CD-ROM, DVD, or flash drive. The boot sequence determines the order in which each drive is accessed when the system is looking for the operating system files. Most systems check the hard drive (usually drive C) first, then they may search optical drives or USB devices. If a system checks the hard drive before any other drive, and a valid operating system is installed on the hard drive, then the system will boot from the hard drive regardless of whether bootable media exists in an optical drive or USB port. If you want to force a system to boot from a drive other than the hard drive, you can change the boot sequence by adjusting the system BIOS. |
| **Basic Input Output System (BIOS)** | BIOS software is built into a computer and is the first code run by a PC when it is powered on. When the computer starts, it performs the power-on self-test (POST), which initializes the system and identifies system devices such as the CPU, RAM, video card, keyboard, mouse, hard drive, optical drive, etc. The next job of the BIOS is to locate boot loader software which loads the operating system (boots the computer). |
| **BIOS setup utility** | Any user can access the BIOS setup utility at startup in order to change the boot sequence, thereby instructing the computer to search the optical drive first, for example. Because the BIOS is built-in, it is accessible before the operating system is loaded. Power the system on, then watch for an "entering setup" message during the first few seconds of startup. The message indicates the key(s) you need to press in order to enter the BIOS setup utility. |
| **ISO image** | A single file that is an "image" of an entire CD, DVD or Blue ray disc. Because an ISO is a complete image, you can download an ISO file from the Internet, or access it on a network, and then burn the image to an optical medium. If the ISO is an image of an installation program, such as for Windows 7, you can burn the image to optical media and then use the media as a boot disc. |

# Removable Media Installation

Most home and small organization installations are performed from removable media, such as a CD, DVD and most recently, a flash drive. The media must be bootable for the installation to proceed, and the computer must be configured with a boot sequence that will check the removable media drive for operating system files.

## DVD

For an end user, installing Windows 7 is a matter of inserting the installation DVD and answering the questions presented during the interactive installation setup procedure. Because the program requires the user to answer questions as the operating system is being installed, this type of installation is referred to as a "high-touch" installation (HTI).

Installing from a DVD can take several minutes to over an hour, depending on the speed of your machine. The computer will reboot automatically when the installation process completes. The following steps describe how to perform a clean installation of Windows 7 from the installation DVD. (If you prefer to perform an upgrade, select *Upgrade* in step 6):

1. Insert the Windows 7 disc into the DVD drive and power on the machine.
2. Select the option to boot from the DVD.
3. Specify your regional settings and click **Next**.
4. Click **Install Now** to start the installation.
5. Read and accept the license agreement, then click **Next**.
6. Select **Custom** to perform a clean install.

7. Click **Next** to allow the installation engine to prepare (format and partition) the hard disk and begin the process of extracting and copying the installation files.
8. After the system reboots, you will be prompted to enter a user name and a computer name. The user account created is automatically an Administrator account. The computer name should be unique on the network. Enter the user name and computer name, then click **Next**.
9. Enter and confirm a password for the user account. You can optionally specify a password hint. (Note that although a password is not required, it is strongly recommended that you add a password to each user account on the machine.)
10. Specify whether you want to configure the system to receive automatic updates from Windows Update. You can postpone the decision by selecting **Ask Me Later**. (You will learn more about Windows Update in a later lesson.)
11. Specify the appropriate data and time zone settings, then click **Next**.
12. If the system is connected to a network, you will be asked to specify the network type (Home, Work or Public). When the installation is complete, the Windows 7 Desktop appears.

## USB

Installing Windows 7 from a flash drive is faster than installing from DVD, and provides a method for installing to a Netbook computer (which usually doesn't include an optical drive). To perform a USB-based installation, you must create a bootable flash drive and then copy the installation files from the original installation DVD onto the flash drive.

The process requires a USB flash drive with at least 4 GB of space. Note that the procedure will completely erase all data on the flash drive.

To make a flash drive bootable, you must open a command prompt window as an administrator and launch the Diskpart utility, which allows you to create and view disk partitions. A command prompt window is a text-based interface you use to interact with the operating system. That is, you enter and execute commands in a non-graphical environment.

To open a command prompt window as an administrator, click **Start**, then type: `cmd` in the Search bar. When the command prompt shortcut appears in the Start menu, right-click it and then select **Run as administrator**.

Enter the following commands by typing the command name and pressing ENTER. These steps will launch the Diskpart utility to make the flash drive bootable:

1. `Diskpart` (launches the utility)
2. `List Disk` (the output from this command will show the number assigned to the USB drive on the system)
3. `Select Disk` *x* (replace *x* with the number assigned to the USB drive. This command selects the USB drive.)
4. `Clean` (removes all information from the USB drive)
5. `Create Partition Primary` (creates a primary partition on the flash drive)
6. `Active` (marks the primary partition as active)
7. `Format fs=FAT32 quick` (formats the flash drive)
8. `Assign` (prepares the USB drive so that it can be assigned a drive letter when you connect it to a system)
9. `Exit` (exits the Diskpart utility)

After you have exited the Diskpart utility, click the close button at the upper-right corner of the command prompt window to close it.

Use Windows Explorer to drag and drop all the files on the Windows 7 installation CD onto the flash drive. The flash drive can now be used as installation media.

## Exercise 1-4: Bootable Flash Drive Demonstration

In this instructor-led exercise, the class will watch a video that demonstrates the steps for creating a Windows 7 installation flash drive.

1. **Instructor:** access and play the video listed below. Note that although the video is 8 minutes long, the pertinent information ends at the 6-minute mark.

   http://www.techrepublic.com/blog/itdojo/video-install-windows-7-from-a-usb-flash-drive/1276

2. How easy (or difficult) was the procedure for creating a Windows 7 installation flash drive?
3. Do you think USB installation media would be beneficial in a corporate environment? Why or why not?
4. If you create a Windows 7 installation flash drive, on how many systems can you install the software?

In this exercise, you watched a demonstration of how to create a Windows 7 installation flash drive.

### Automated Installations

Because the interactive installation process is time-consuming and would be impractical for deploying Windows on a large number of systems, Microsoft provides tools and methods for automating the installation process. Automated installation strategies use an answer file, which is an Extensible Markup Language (XML) file that provides answers to the questions asked during installation. The Microsoft Automated Installation Kit (AIK) provides tools for creating answer files.

#### High Touch with Standard Image

This strategy involves creating a customized installation image for the new systems. Typically, this customized image includes settings, device drivers, installed applications, etc. Using a customized image for clean installs allows the IT staff to deploy systems more quickly. This strategy is recommended for companies with an IT person on staff and an unmanaged network of between 100 to 200 computers.

#### Lite Touch Installation (LTI)

Lite touch installation requires that the technician manually boot the system and begin the installation. The answer file provides the answers to the questions and the installation proceeds unattended. This deployment strategy is recommended for organizations with a dedicated IT staff and a managed network with between 200 and 500 client computers.

#### Zero Touch Installation (ZTI)

Zero touch installation does not require any physical interaction from the technician. The entire process can be started from a network server. This deployment strategy is recommended for organizations with managed networks of 500 or more computers, and an IT staff with advanced network management, configuration and deployment skills.

ZTI requires substantial infrastructure – Active Directory Domain Services (AD DS), Microsoft System Center Configuration Manager (SCCM), and the Microsoft Deployment Toolkit (MDT).

## Network-based Installations

Network-based installations are performed from network shares or special installation servers running Windows Deployment Services (WDS).

To perform an installation from a network share, you must install the Microsoft Deployment Toolkit (MDT) which includes tools for creating the shares, creating answer files and importing and customizing installation images. The MDT creates a custom Windows Preinstallation Environment (PE) boot disc that can be used to boot a computer and install the operating system from the network.

The Windows PE is a minimal operating system with limited services that is used to prepare a computer for Windows installation, to copy disk images from a network server, and to initiate Windows Setup.

When WDS is used for network-based installation, a custom image of the operating system is created and imported into the WDS server. Client systems are booted and then the custom image is installed. Client systems can be booted manually using a boot disc, or they can be connected to the network via specialized Preboot Execution Environment (PXE) –compliant adapters. A PXE-compliant network adapter allows a client system to boot from a server on the network.

### Network versus Cloud-based Deployment

Cloud-based computing is computing that uses the Internet to provide its network infrastructure. That is, applications, storage space, and computer management consoles can be housed on Internet servers instead of being housed on an organization's privately-owned equipment.

Cloud-based services are leased monthly through a subscription service with a cloud provider. Microsoft's cloud solution is called Windows Intune, which allows you to centrally manage and secure all your PCs through a Web-based console.

Cloud-based management services allow the IT manager to monitor, update, and manage PCs without the requirement of building and maintaining a server-based network infrastructure. All that is required is an Internet connection, installation of the Intune client software on each PC that is to be managed, and a subscription to the service.

IT managers can deploy software installations, patches, and upgrades to managed PCs using the cloud-based service. Client systems need only be connected to the Internet; users do not even have to be logged on to the machines. Cloud-based deployment supports users scattered around the planet.

# Introducing Virtualization

Objective 2.4 3.5

In the context of computing, the word *virtual* refers to the way a particular component or environment appears to a user. For example, a *virtual machine (VM)* is a software implementation of a computing environment that executes programs like a physical machine. That is, a VM is a simulated collection of computer hardware that exists and behaves like a real (physical) computer. You create a VM using virtualization software.

The machine that runs the virtualization software is the host. Each VM running on the host can run its own guest operating system and application software. The guest operating system and application software will function exactly as if they were installed on a physical computer system.

The host machine stores and provide resources to VMs which run on it. Therefore, each VM will have a CPU and RAM to perform computations, a keyboard and mouse connection, a display driver for the monitor, and a network interface card (NIC) to connect to the network. You can also specify the size of a (virtual) hard drive, and decide to connect an optical drive, and USB ports.

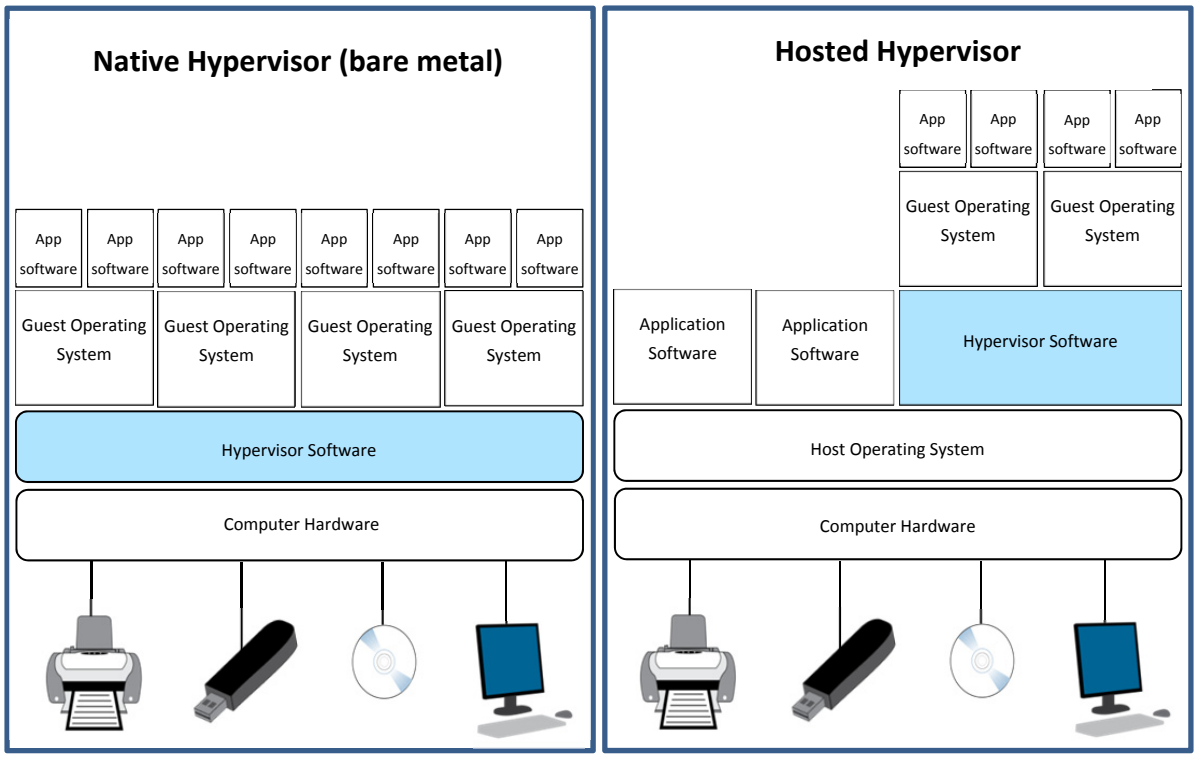
## Hypervisor

**MMM**
Virtual Machines – an Extended Discussion

The software that runs the virtual machines is called a *hypervisor*. There are two types of hypervisors:

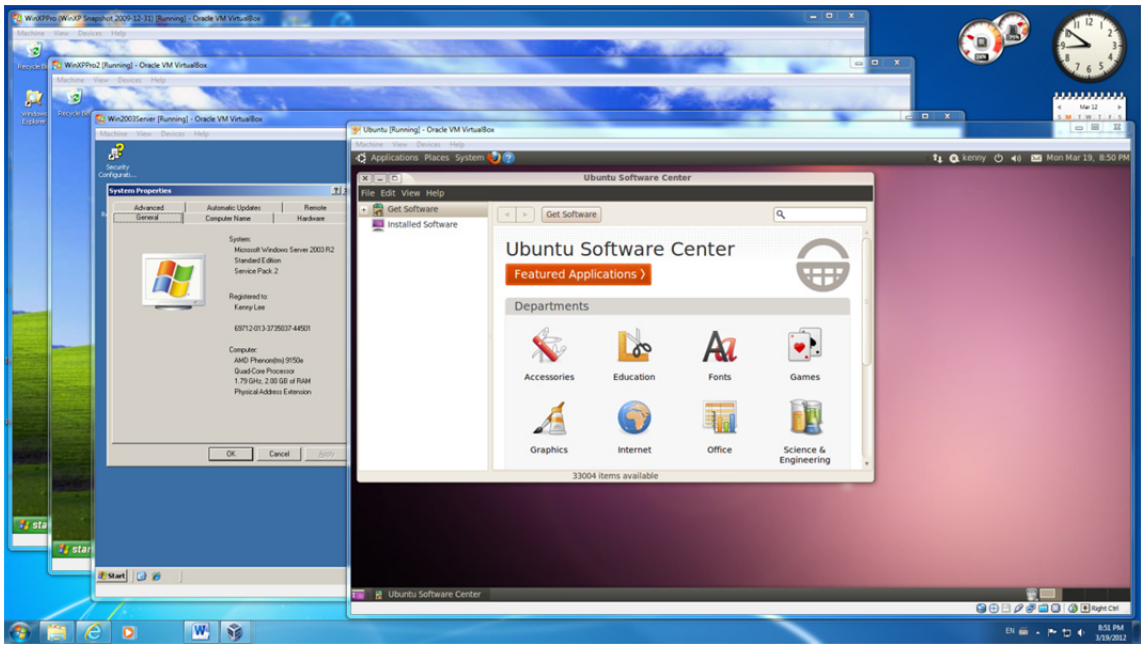
- *bare metal* (Type 1), and
- *hosted* (Type 2)

A hosted hypervisor is like any other application software that runs on top of an operating system. Examples of hosted hypervisors are Microsoft Virtual PC, Microsoft Server, Oracle VirtulBox, and VMware Server. A bare metal hypervisor is designed to run exactly as the name implies: directly on top of the computer hardware without an operating system in between. Examples are: Microsoft Hyper-V Server, VMware ESX, and Citrix XenServer.




Each hypervisor is able to run one or more guest operating systems (e.g., UNIX, Linux, Mac OS X). The only limitation imposed on the operating system is that it must be compatible with the virtual hardware created by the hypervisor. The maximum number and type of guest operating systems that can be supported is only limited by the amount of RAM and the number of CPU cores on the host machine.

The following screenshot shows a hypervisor software called VirtualBox running on top of Windows 7. The VirtualBox is running four guest operating systems at the same time: two different Windows XP machines, one Windows Server 2003 machine, and one Ubuntu (Linux) machine.



Microsoft offers two virtualization products with Windows Server 2008 and Windows 7:

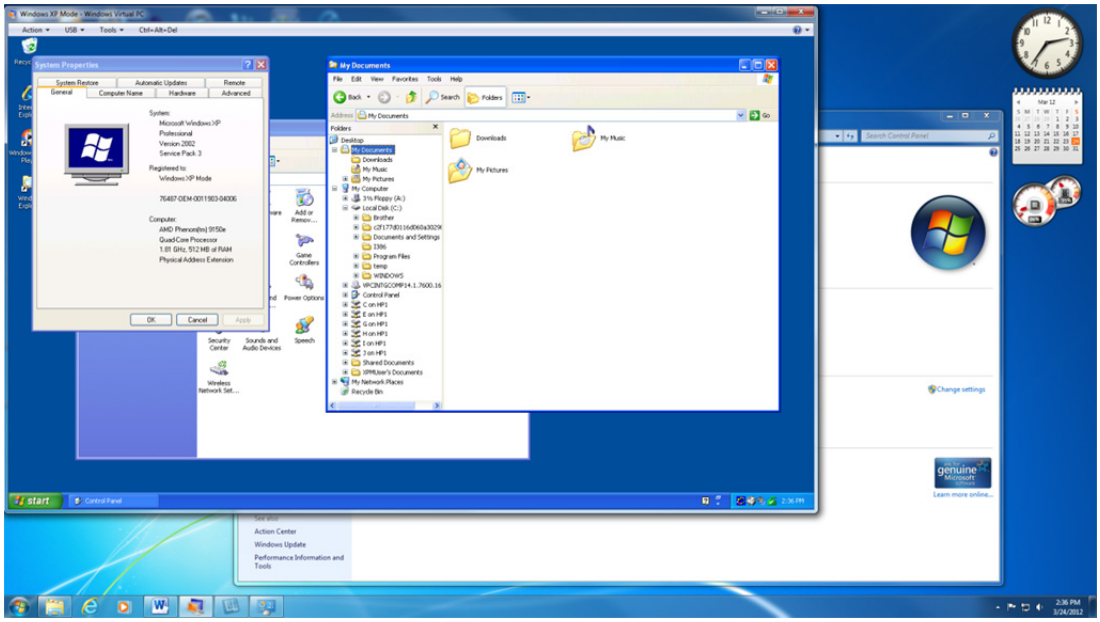
| | |
|---|---|
| **Hyper-V** | Runs on Windows Server 2008 and Windows Server 2008 R2 and runs VMs for an enterprise. Hyper-V does not run on Windows 7, but can run Windows 7 as a guest operating system within a VM. |
| **Windows Virtual PC** | Runs VMs on all editions of Windows 7 and is an optional component that can be freely downloaded and installed. Windows Virtual PC can be used to run properly-licensed versions of Windows Vista, Windows 7 or Windows XP in a virtual environment. Windows Virtual PC is required to run Windows XP Mode (which you will read about in the next section.) |

## XP Mode

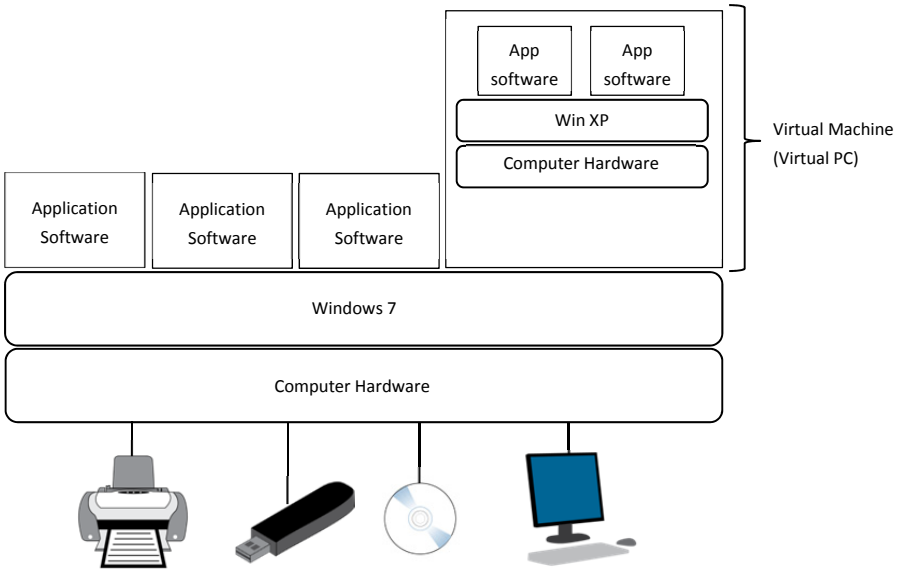
New in Windows 7 is a feature called *XP Mode*, which enables you to create and run a Windows XP virtual machine on your Windows 7 Desktop. Any application software installed inside a VM functions as though it is installed on a physical machine, but interacts only with the virtual environment. By installing legacy applications in the Windows XP virtual machine, you are able to run application software that runs correctly in Windows XP, but is unable to run in Windows 7.

In other words, Windows XP Mode is used to allow applications that will not run on Windows 7 natively to run in a VM on your Windows 7 computer. When an application runs in Windows XP Mode, you see the application windows on your local Windows 7 Desktop as if it were running locally, but it is actually running in a background Windows XP VM.

The following screenshot shows the Windows XP Mode running on the Windows 7 Desktop:

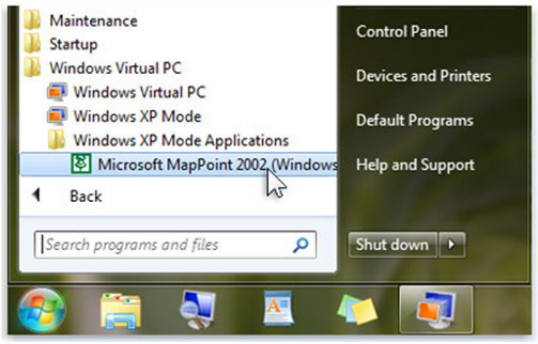


Once running in XP Mode, your application software will have access to all peripherals on the computer. For example, when you install your software in XP Mode, you can insert the installation DVD in your real computer's DVD drive, and the Virtual PC software will be able to connect to it. Similarly, you can access USB ports and send output to printers that are actually connected to the underlying physical computer. The Virtual PC performs all of the work of creating and maintaining these connections between XP Mode and the physical computer.




Keep in mind that you will most likely need a separate software license for any application you install in XP Mode. From a licensing point of view, a VM is a computer separate from (even though it is running on) your physical computer. For example, you will need two licenses of MS Word if it is already installed in Windows 7, and you want another copy in XP Mode.

Software applications installed in XP Mode will appear under the Windows XP Mode Applications folder in the Start, All Programs menu. This arrangement makes it easier for users to see what applications are available on both their physical Windows 7 system and their Windows XP Mode virtual machine.




## Installation and Requirements

Windows XP Mode is a special version of the Windows XP Professional (SP3) operating system designed specifically to run on Windows 7 as a guest operating system. Windows Virtual PC must be installed on the Windows 7 system in order for Windows XP Mode to run.

Note that while Windows Virtual PC will run on all editions of Windows 7, XP Mode is supported only in the Professional, Ultimate and Enterprise editions. (You can, however, install Windows Virtual PC on a lower edition of Windows 7 and then install a purchased, licensed copy of Windows XP or any other operating system and run it as a guest operating system in a VM.)

Windows XP Mode is an optional component of Windows 7 and is available for download free of charge at http://www.microsoft.com/windows/virtual-pc/default.aspx**.** No license is required to run Windows XP Mode.

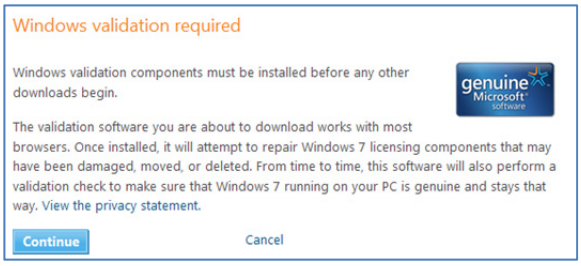
It is possible run Windows XP Mode on a computer with as little as 1 GB of RAM. However, for optimal performance the system should have at least a 4 core CPU, 4 GB RAM, and a 7200 rpm hard drive or SSD. Using an under-powered system as the host can cause application software to perform slowly or inconsistently because of the extra processing power required to run the VM itself.

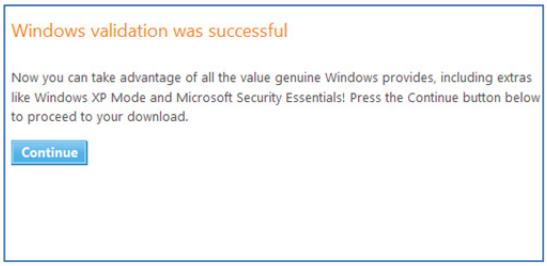
# Exercise 1-5: Installing Windows Virtual PC and XP Mode

In this exercise, you will download and install Windows Virtual PC and XP Mode.

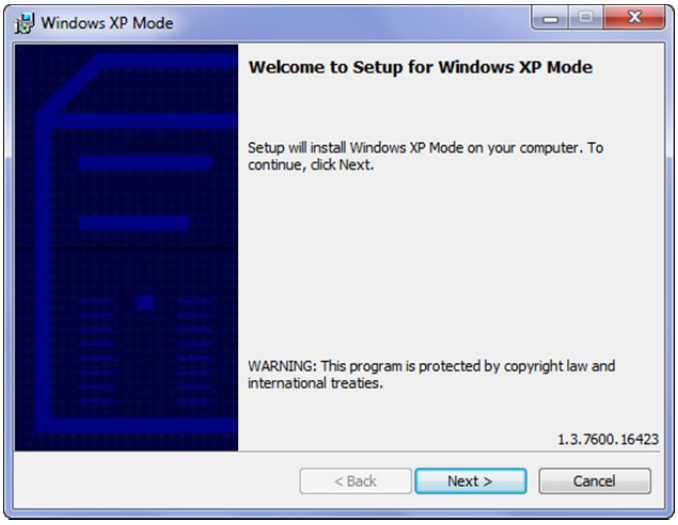
First, you will check to see if Windows Virtual PC and XP Mode came pre-installed on your system.

1. If necessary, power on your system and log on using an Administrator account. Click the **Start** button, click **All Programs**, then scroll the list to see if Windows Virtual PC is listed. If not, then you will need to install it.
2. Click in an open space on the Desktop to close the Start menu, then open a Web browser and navigate to http://www.microsoft.com/windows/virtual-pc/default.aspx.
3. On the Windows Virtual PC Web page, click the **Get Windows XP Mode and Windows Virtual PC now** button.
4. On the Web page, use the drop-down lists to specify your edition of Windows 7 and the desired language for the installation.
5. Scroll down until you see Step 2 Windows XP Mode, then click the blue **Download** button below Windows XP Mode to begin downloading the application. It is a large file, and may take several minutes.
6. You may be prompted to validate your version of Windows. If you are, click the **Continue** button, wait for the Windows validation was successful message, then click the **Continue** button once more.

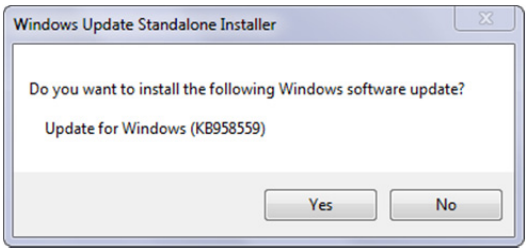


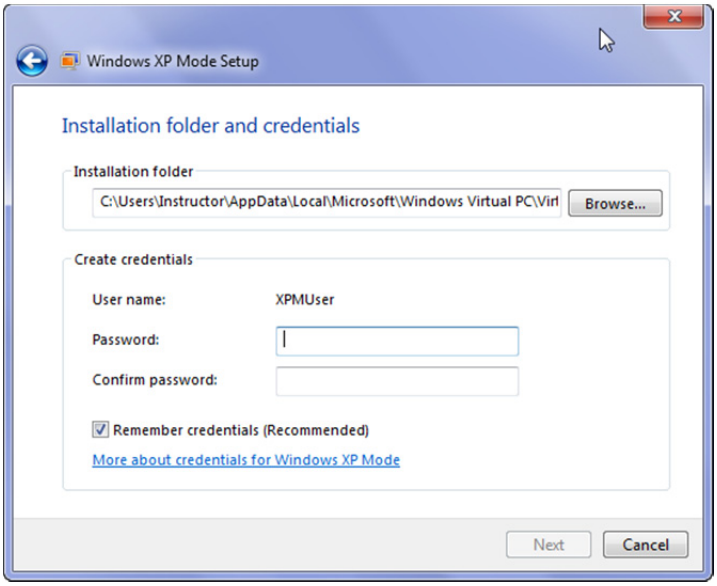

7. When prompted to run, save or cancel the executable file, click **Run** to start the Windows XP Mode setup wizard.



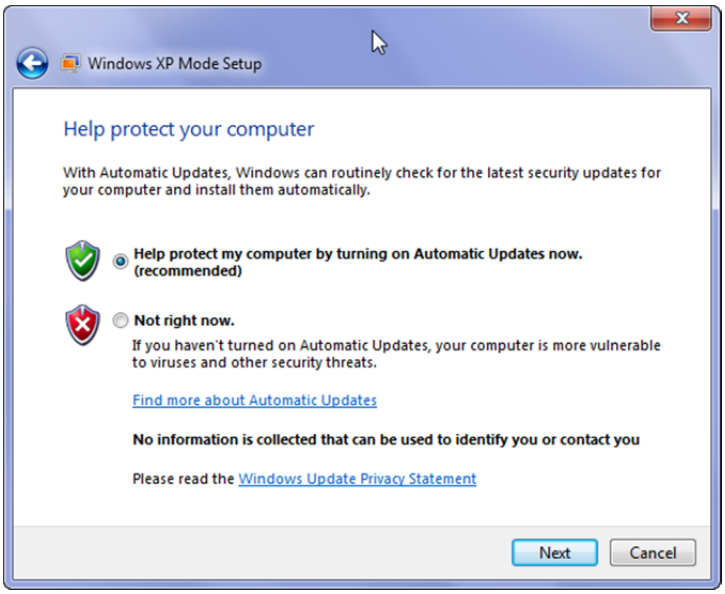

8. Click **Next** twice, then click **Finish**.
9. On the Windows Virtual PC Web page, locate Step 3 Windows Virtual PC, then click the blue **Download** button below Windows Virtual PC and click **Open** to begin downloading and installing the application.




10. When prompted to install the software update, click **Yes**.
11. Click **I Accept** to accept the license agreement and install the update.
12. When the installation is complete, click **Restart Now** to restart the computer.
13. Log back onto the system using an Administrator account.
14. Click **Start**, click **All Programs**, then click **Windows Virtual PC** to make sure that Windows XP Mode displays in the Start menu.
15. In the open Start menu, click **Windows XP Mode** to begin configuring XP Mode. You will need to configure XP Mode to ensure it functions properly.
16. Accept the license terms and click **Next** to view the Installation folder and credentials screen. By default, the user name is set to XPMUser.



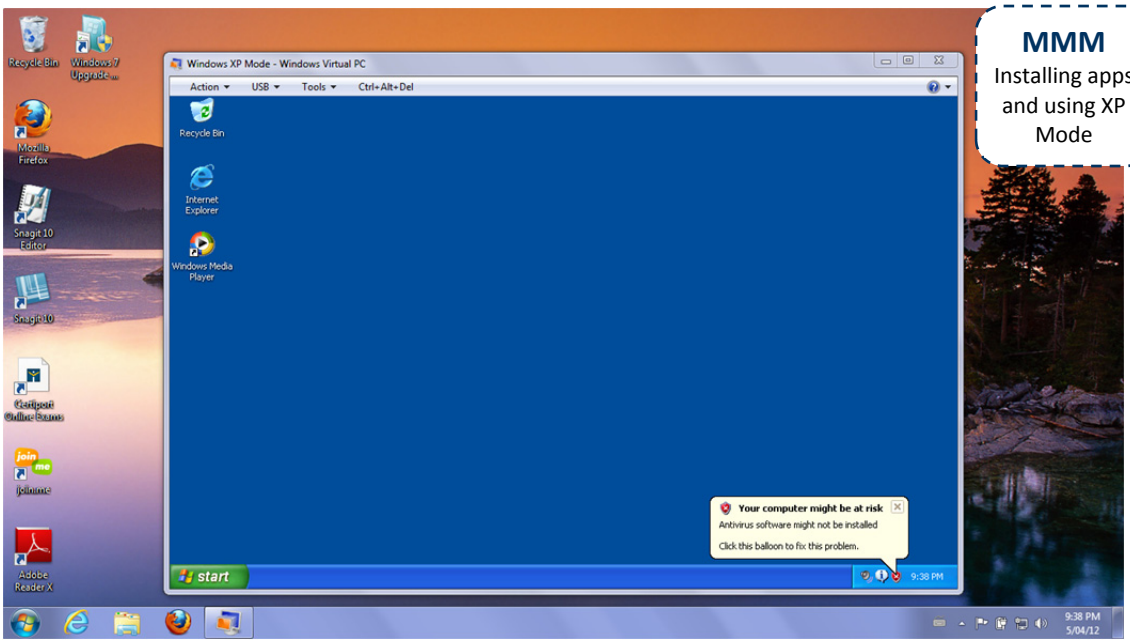

17. Specify and confirm a password. If you leave the Remember credentials (Recommended) option selected, you will not need to enter the password when you use XP Mode. Click **Next**.




18. Select **Help protect my computer by turning on Automatic Updates now. (recommended)**. Windows XP Mode relies on the Windows Update service to obtain updates for Windows XP with SP3. To ensure that Windows XP with SP3 receives updates, both the host computer and the virtual machine must be connected to the Internet—and the Windows Update service must be configured in the virtual machine that runs Windows XP Mode. Click **Next**.
19. Next you must share the drives on the physical computer with Windows XP Mode.


20. Click **Start Setup**, then wait while Windows sets up XP Mode on your system. This process can take several minutes. When setup is complete, Windows XP Mode will appear as a window on your Windows 7 Desktop.

**MMM**
Installing apps and using XP Mode




21. Click the close button in the upper-right corner of the Windows XP Mode window to put XP Mode into hibernation.

In this exercise, you installed and set up Windows XP Mode.

## MED-V

Objective 3.5

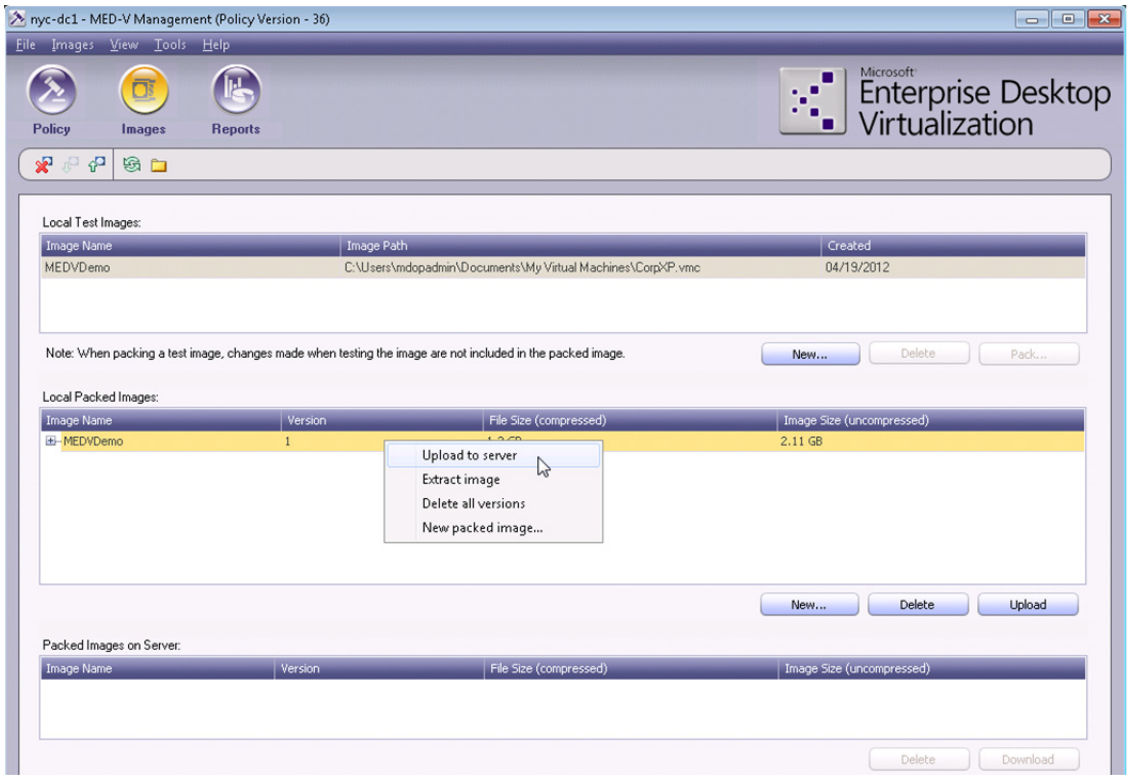
Microsoft Enterprise Desktop Virtualization (MED-V) is essentially an enterprise-wide version of the XP Mode in Windows 7. It is packaged together with other products as part of the Microsoft Desktop Optimization Pack (MDOP).

Like Windows XP Mode, MED-V allows enterprise users to continue using applications that were designed to run in (32-bit) Windows XP, but are incompatible with Windows 7 to some degree or another. MED-V eliminates conflicts and allows older applications to run well on Windows 7.

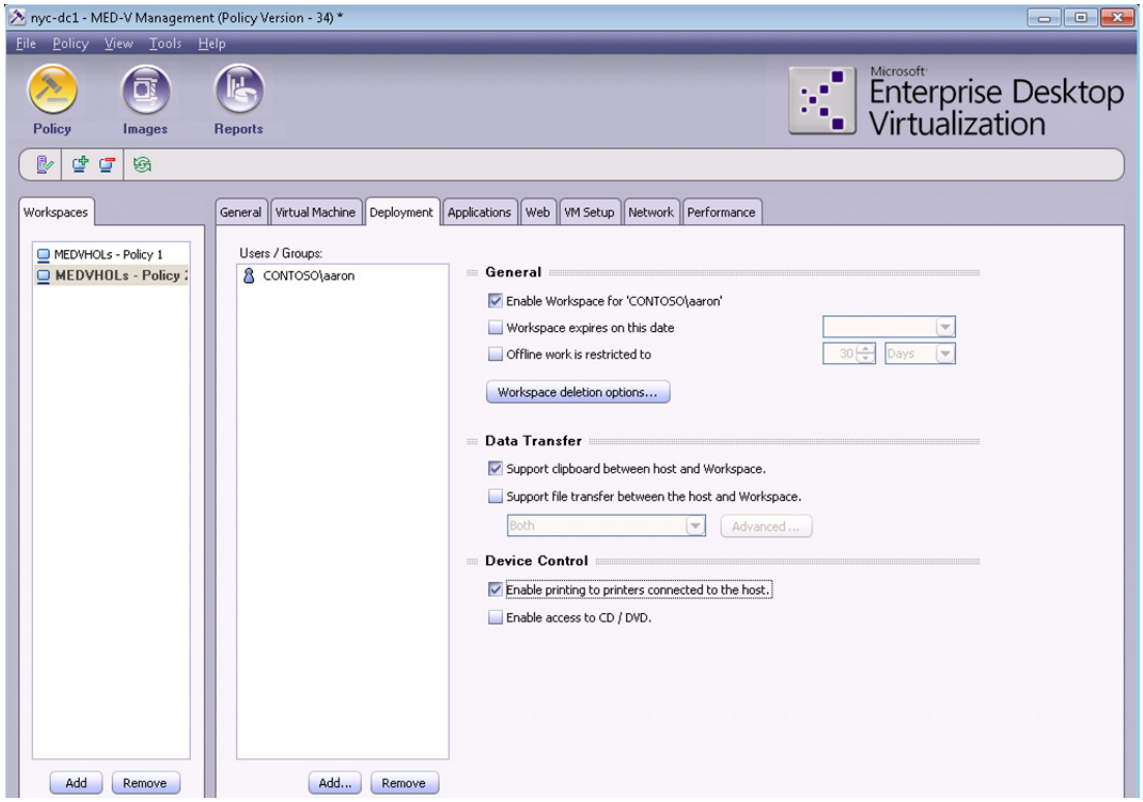
MED-V is designed for enterprises; it allows you to use a centralized system management tool to create, configure, and deploy virtual Windows machines (called *workspaces*) to end user computers. This is a tremendous advantage over using XP Mode, as it would be very time-consuming to manually install and configure XP Mode on every user's computer.

A typical large enterprise may include thousands of users. To help organize and manage all those users, it makes sense to define groups of users who have common needs and use a common group of applications. For example, all users in the Accounts Payable department likely need access to several treasury and payment applications, and it therefore makes sense to create an Accounts Payable users group.

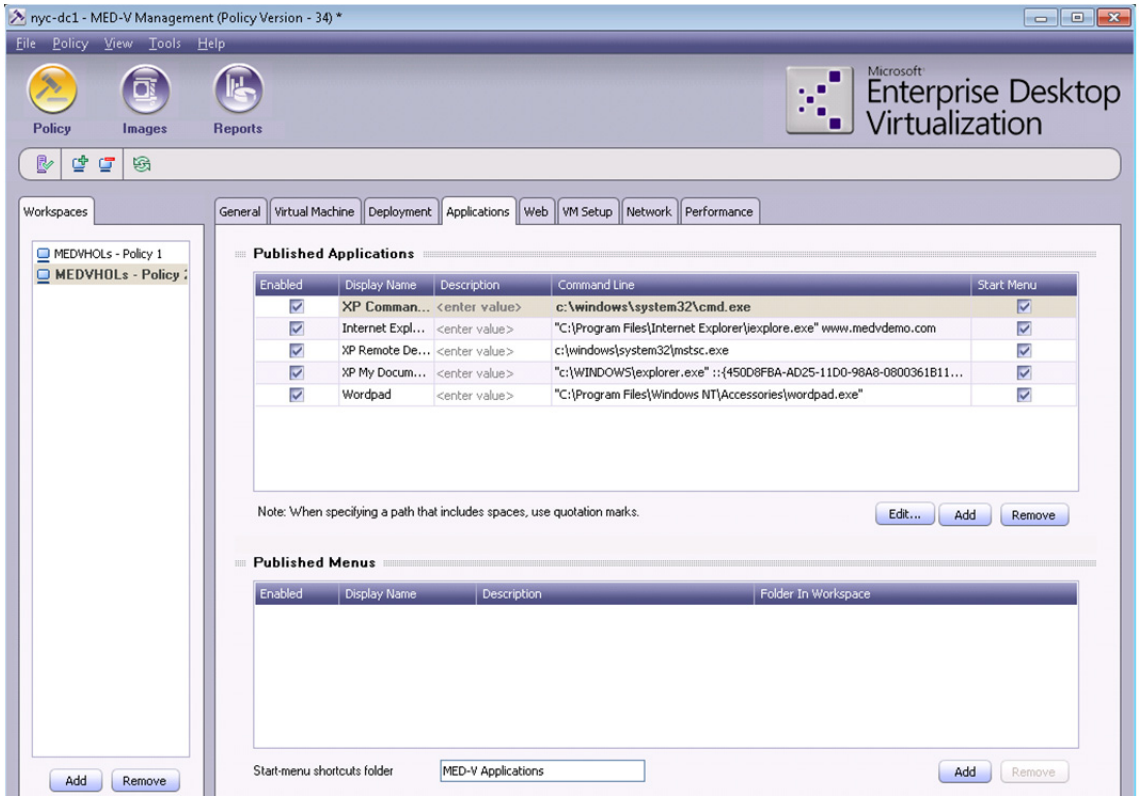
In MED-V, you create an *image* of a virtual machine (VM) and upload it using the Microsoft Enterprise Desktop Virtualization (MED-V) Management Console. You can think of an image as a template or a master copy; when a user is set up to use MED-V, the central server will create a new workspace by copying the image down to the user's local computer. All Accounts Payable users would then have an A/P workspace on their computer – that is, a copy of the A/P MED-V image. Sales users, on the other hand, would have their own Sales workspace.



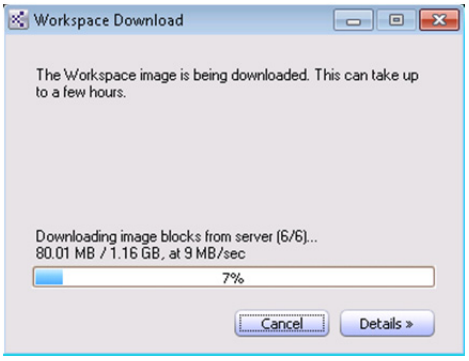

Each image is further configured to identify which users are permitted to access this image. This setting is known as a *usage policy*, and is stored in Active Directory. This will ensure that the Sales users cannot download the A/P image onto their computers, for example.



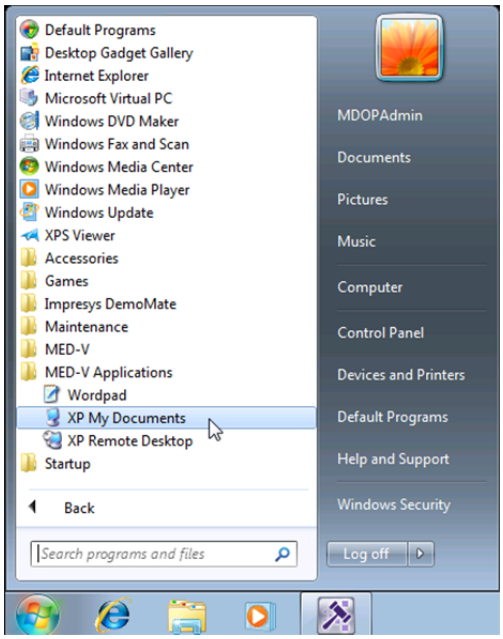
The MED-V image is then configured to run selected applications, as shown in the following screen capture.




When a user is set up to access his or her MED-V workspace, the image is downloaded to his or her local machine as shown in the following screen captures.

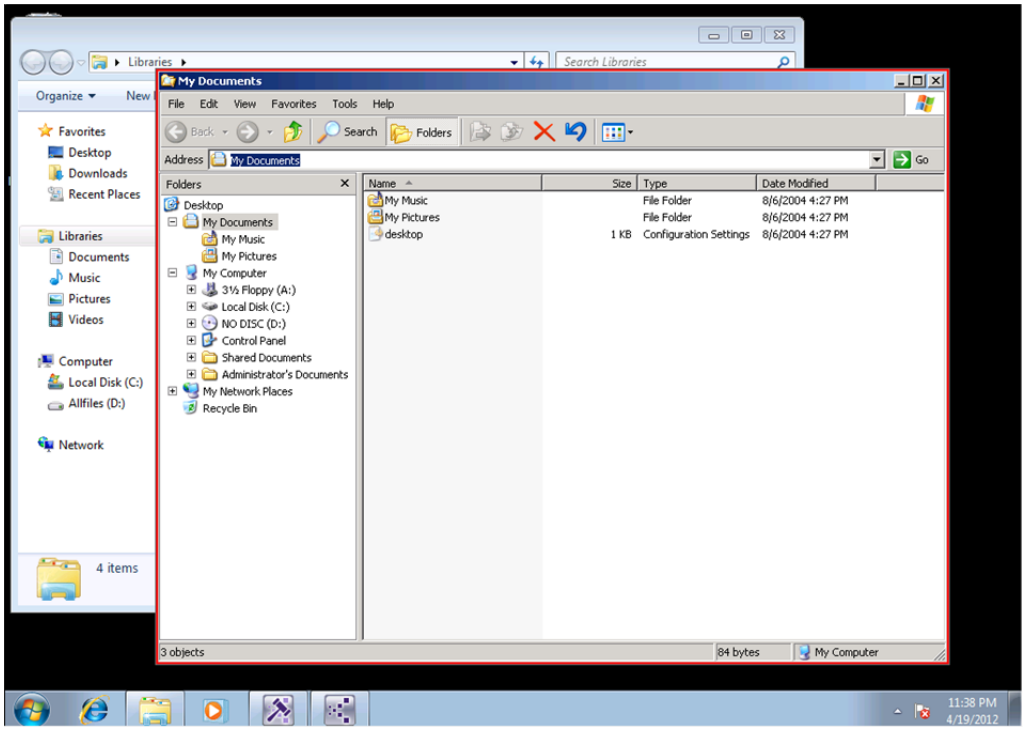




Once installed, MED-V applications will simply appear in the **Start**-**All Programs** list, under the **MED-V Applications** folder. These applications can also be configured as individual shortcuts appearing at the top of the **All Programs** list.




When the MED-V administered software starts up, a border will appear around the application window to indicate that it is running under MED-V. Other than that indicator, a user cannot easily detect that the software is running in a virtual machine.

Microsoft has pursued seamless integration in other ways to make MED-V easy to use. For example, printers will appear in the application as if they were installed on the local machine. Similarly, the local *My Document* folders and USB drives will also appear when users open and save data files. To access or save data files located in other locations such as on networked drives, the user must use the File Transfer tool to move files to and from the virtual PC workspace.



Specific URLs (e.g., *finance.companyname.com*) can also be reserved to automatically run under MED-V instead of the default web browser installed on the user's computer. This capability is very useful because many software vendors offer a web front-end for their applications. Like WinXP applications, these web pages may be incompatible with the newer version of Internet Explorer.

For example, suppose you open the current version of Internet Explorer in your Windows 7 machine and enter the address of the website for your corporate finance system. MED-V can be configured to intercept this address, start up an older version of Internet Explorer and load the finance system for you in a separate window. Again, this seamless integration relieves you from having to remember which websites must run on older web browsers.

One of the Microsoft websites offers a hands-on demonstration (called virtual labs) of setting up, managing, and using MED-V. Go to http://technet.microsoft.com/en-us/virtuallabs/ and click the Windows 7 link.

# Lesson Summary

In this lesson, you learned how to plan for an operating system upgrade, about the various Windows 7 editions and installation options and about how virtualization can support legacy applications in Windows 7. You are now able to:

- ☑ Explain the difference between 32-bit and a 64-bit operating systems.
- ☑ Describe the Windows 7 operating system editions, including features, availability and minimum requirements.
- ☑ Identify upgrade paths from various versions of Windows to Windows 7.
- ☑ Explain the function and characteristics of Windows Anytime Upgrade.
- ☑ Understand hardware and software compatibility issues and explain why upgrading to Windows 7 requires planning.
- ☑ Use the PC Upgrade Advisor.
- ☑ Use the Windows 7 Compatibility Center to check for software and hardware compatibility issues.
- ☑ Explain the difference between an in-place upgrade and a clean install.
- ☑ Explain different types of installation strategies, including High Touch installation, High Touch with Standard Image, Lite Touch installation and Zero Touch installation.
- ☑ Understand media-based and network-based installations.
- ☑ Explain cloud-based software deployment.
- ☑ Explain the purpose and advantages of virtualization.
- ☑ Explain the function and characteristics of Windows XP Mode.
- ☑ Explain the function and characteristics of MED-V.

**MMM**
Go online for Additional Review and Case Scenarios

# Review Questions

1. In order to make changes to a system that will affect other users, you must be logged on with a(n):
   a. power account
   b. standard user account
   c. administrator account
   d. guest account

2. Windows XP mode is supported in which Windows 7 edition(s)?
   a. Starter, Home Premium and Enterprise
   b. Professional, Ultimate and Enterprise
   c. Enterprise only
   d. Professional only

3. What is the amount of RAM required to run Windows 7 Home Premium 64-bit?
   a. 1.0 GB
   b. 2.0 GB
   c. 3.5 GB
   d. 4.0 GB

4. The software that runs the virtual machines on a server is called:
   a. hypervisor software
   b. Remote Desktop software
   c. ISO software
   d. cloud deployment software

5. Which of the following Windows 7 installation strategies requires substantial network infrastructure, Active Directory Domain Services, and Microsoft System Center Configuration Manager (SCCM)?
   a. High Touch Installation
   b. High Touch with Standard Image
   c. Lite Touch Installation
   d. Zero Touch Installation

# Lesson 2: Operating System Configuration

## Lesson Objectives

In this lesson, you will learn to configure various operating system components and features including Control Panel options and Desktop settings. You will also learn about native applications and tools, and learn how Windows supports mobility. By the completion of this lesson, you will be able to:

- ☐ Identify the features and components of the Windows 7 Desktop.
- ☐ Understand how to navigate a breadcrumb trail.
- ☐ Identify the features and components of the Windows Explorer window.
- ☐ Add and configure Desktop gadgets.
- ☐ Describe and access user profile folders.
- ☐ Configure display settings, including screen resolution and screen magnification and configure Windows 7 to support multiple display devices.
- ☐ Create and modify Desktop shortcuts, create Start menu shortcuts, and add system icons to the Desktop.
- ☐ Use Aero features for window management.
- ☐ Modify and apply Aero themes.
- ☐ Use the Snipping Tool.
- ☐ Describe the major features of Internet Explorer.
- ☐ Describe the Windows Media Center.
- ☐ Describe Windows Media Player.
- ☐ Configure administrative tools.
- ☐ Configure accessibility options.
- ☐ Describe how to use MSCONFIG.
- ☐ Explain the Windows Sync Center.
- ☐ Explain the Windows Mobility Center.

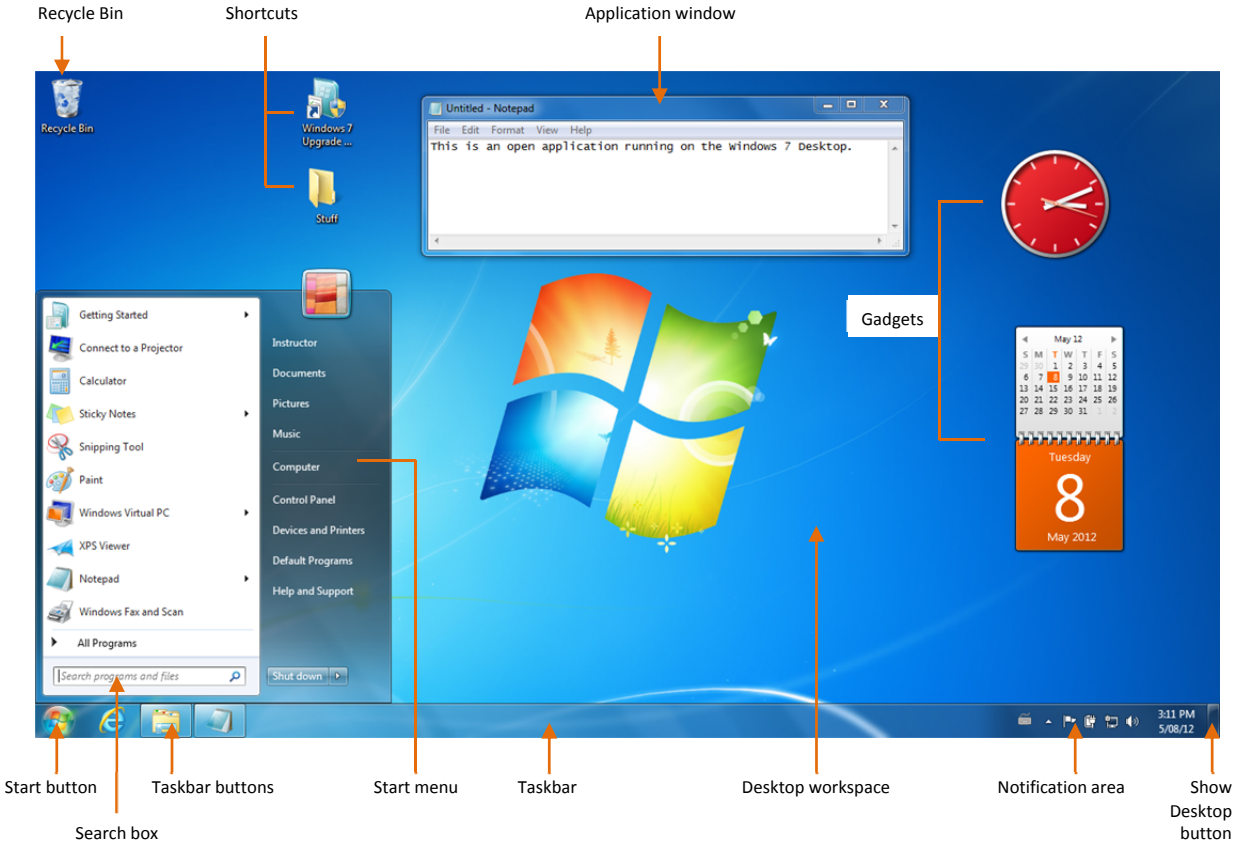
### Exam Objectives

1.1 Configure Control Panel options
1.2 Configure desktop settings
1.3 Understand native applications and tools
1.4 Understand mobility

# Introducing the Desktop

In this lesson, you will learn how to configure Windows 7 to enable users to work productively and comfortably. You will begin by examining the Windows 7 Desktop.

The Windows 7 Desktop is the main interface for the end user. It includes a Start menu, Desktop icons, shortcuts and gadgets. The Desktop is also the place where applications run.




The Desktop includes the following features:

| | |
|---|---|
| **Start button** | The Start button opens the Start menu. You can click the Start button or press the Windows logo key on your keyboard to open the Start menu. |
| **Start menu** | The Start menu is the gateway to access programs, files, folders and settings. You also use the Start menu to search for files, folders and programs, get operating system Help, log off or switch to a different user, or turn off the computer. The Start menu includes three basic parts: the left pane, the right pane and the search box. The left pane shows a short list of programs. You can click All Programs at the bottom of the left pane to open a complete list of programs. The right pane provides access to commonly used folders, files settings and features, and you use the right pane to log off, switch users or power off the computer. |
| **Search box** | You can use the Start menu search box to quickly access programs, documents, folders or system components. Click in the search box and start typing a keyword for what you want to find and Windows displays a categorized list of relevant folders, files, programs and components. You can click a category to search only items within the category, or click the See more results link at the bottom of the list.<br>You can also run a program by entering its name into this box. |

| | |
|---|---|
| **Taskbar** | The Taskbar is the long horizontal bar at the bottom of the screen. It includes three main sections: the Start button, the middle section (which displays the taskbar buttons for open programs and files), and the notification area (which includes a clock and icons that communicate the status of certain programs and computer settings). |
| **Taskbar buttons** | When you open a program, folder or file Windows creates a corresponding button on the Taskbar. The button shows an icon that represents the open program. When several files for applications are open, the highlighted button on the taskbar indicates the file or application that is currently active. If several files are open within the same program (for example, if you have three open Word documents), you can point to the taskbar button to switch to another open application, click its taskbar button to see a thumbnail preview of its open documents, and then click the thumbnail of the document you want to make active. (Note: The thumbnail preview is available only if your computer supports the Aero interface and if you are using Windows 7 theme.) You can rearrange taskbar icons by dragging them. You can also pin your frequently-used programs to the Taskbar for easy access. |
| **Notification area** | The notification area is at the far right end of the Taskbar. It includes a clock and icons that communicate the status of certain programs and computer settings. For example, the network status and volume control icons display here. When you point to an icon, its name or the status of its setting will appear. You can double-click an icon to open the program or setting associated with it. Occasionally, an icon will display information in a pop-up window (called a notification) to inform you of something. For example, a notification will display when you connect a USB device, or when Windows has installed updates. You can manually close the notification, or wait for it to fade from view. Windows hides icons in the notification area when you have not used them in a while. You can click the Show Hidden Icons button to temporarily display the hidden icons. |
| **Show Desktop button** | The Show desktop button is a rectangular bar at the far right end of the taskbar. It provides quick access to an uncluttered Desktop. You can point to it to make all open windows transparent, so you can see the Desktop for a moment. Or you can click it to instantly minimize all open windows on the Desktop. You can restore all the windows to their previous state by clicking it again. |
| **Desktop workspace** | The Desktop workspace is the empty area on the Desktop on which you can place icons, shortcuts and gadgets. You can also customize this area with Wallpaper. |
| **Shortcuts** | Desktop shortcuts are links to applications, folders or documents the user can access quickly. Often when you install a program, you are asked whether the installer should create a Desktop shortcut. Desktop shortcuts include a blue arrow in the lower-left corner. You can manually create Desktop shortcuts to folders and files. |
| **Gadgets** | Gadgets are mini programs that provide information and easy access to frequently used tools. Calendar, Clock, CPU Meter, Currency, Feed Headlines, Picture Puzzle and Slide Show are the gadgets that come with Windows 7, and you can find more online. In Windows Vista, gadgets were lined to a sidebar and could not be placed anywhere on the Desktop. In Windows 7 gadgets are managed by an application named Sidebar, but can be placed anywhere on the Desktop. |
| **Application window** | Applications run on the Windows Desktop in their own windows. At any given time an application can be in one of three states: minimized, maximized or restored. When an application window is maximized, it completely covers the Desktop and only the Taskbar remains visible. When an application is minimized, it is no longer visible on the Desktop, but you can access it quickly by clicking its button in the Taskbar. When an application window is restored, it is constrained to a size that does not completely cover the Desktop. The application window shown in the preceding figure is in a restored state. Nonstandard applications, such as full-screen games or videos, may completely cover the Desktop and the Taskbar. |
| **Recycle Bin** | The Recycle Bin exists on each internal hard drive in the computer and is a hidden folder into which deleted files are copied, allowing you to restore them at a later time if you decide you want to keep them. The Recycle Bin is a system component and is the only icon automatically placed on the Desktop after installing Windows 7 (unless you customize the installation process with an answer file). A Desktop icon appears different than a shortcut; it does not include a blue arrow. |

# What Lies Beneath

While users interact primarily with the Desktop, it is important to understand that the Desktop is an interface. It provides a single location from which a user can launch programs or open files regardless of where they are physically stored on the hard drive.

## Review of File Storage Basics

All computer information is stored on some medium, usually disks, and the operating system is almost always stored on a hard drive. In computers that use one operating system but contain more than one hard drive, the operating system is installed on one drive only – typically drive C. The hard drive on which the operating system is installed is called the *system drive*.

Information stored on a disk is organized into files. For example, a photograph is stored as a file, a song is stored as a file and a letter is stored as a file. These files can be organized into folders, similar to how folders might be organized in a filing cabinet to enable you to keep all associated data in one place.

When you need to organize your files further, you can create folders, called subfolders, within folders. Subfolders enable you to organize your information hierarchically so things are easier to find when you need them.

This organization of folders is called a *directory* or a directory tree. As the folder structure gets more complex, it begins to resemble the branches of a tree. The highest level of any directory is called the root folder, or the *root directory*.

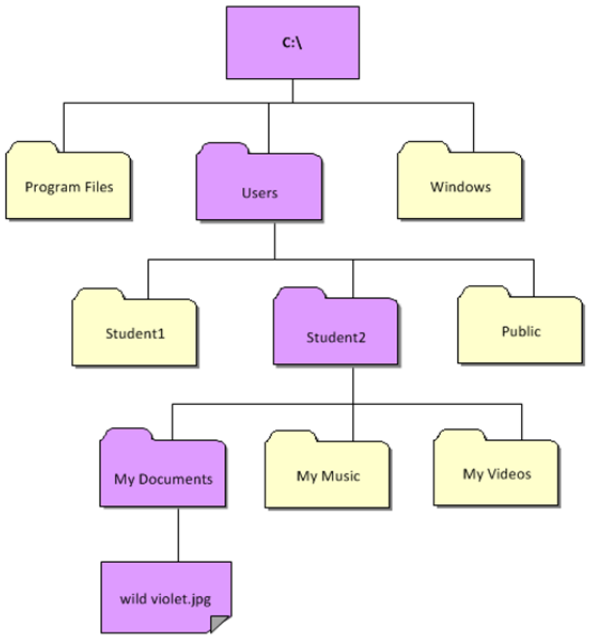
Every file on a computer is stored in a particular location, and that location is described by its path. For example, if drive C has several folders and subfolders, and a file named README.txt is stored on the C drive but is not stored in any of the folders, (that is, the file README.txt is located on the root directory of Drive C), the path to the file is: C:\README.txt.

A file path always begins with the drive letter at the root of the disk, and follows the hierarchy of folders leading to the file. Within the path, the folders in the hierarchy are separated by a backslash (\).

For example, consider the following file path:

**C:\Users\Student2\My Documents\wild violet.jpg**

The path describes the location of the file and how to move through the directory in order to find it. You would start at the root directory; go to the Users folder, then to the Student2 subfolder, to the My Documents subfolder, to the file. This path is illustrated below:




The image used to illustrate the file path includes other folders. There are numerous folders and subfolders on a Windows 7 system, and you can use Windows Explorer to see how they are laid out.

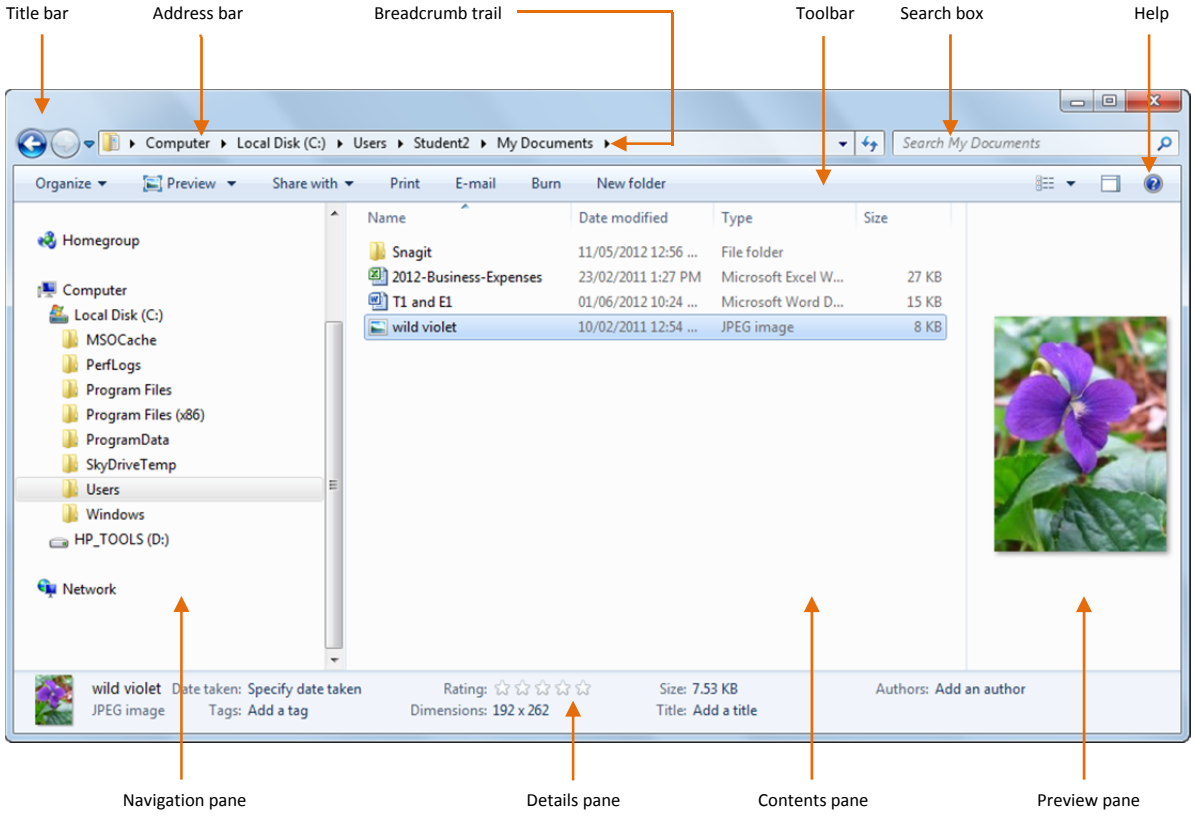
## Breadcrumbs

A navigation aid used in Windows Vista and Windows 7 is the breadcrumb trail. It represents the hierarchy of folders and each part of the trail is an active control. The backslashes of the conventional file path are replaced by arrowheads that provide access to any lower branch of the directory tree. The following figure is the breadcrumb trail for the (conventional) file path **C:\Users\Student2\My Documents**.


# Windows Explorer

Windows Explorer is the tool to use to navigate the directory structure of any disk or drive. It is also the file and folder management system for Windows. You should already be familiar with Windows Explorer; however the following diagram reviews the terminology for referring to particular parts of the window.

The following figure shows the main panes of the Windows Explorer interface.




Windows Explorer includes the following features:

| | |
|---|---|
| **Title bar** | You can drag the title bar to move the window to another location on the Desktop. |
| **Address bar** | Displays a breadcrumb trail (also called an eyebrow menu) of drives and folders leading up to the folder you are viewing. The name of the folder you are currently viewing appears at the end of the trail. |
| **Breadcrumb trail** | Represents the hierarchy of folders in a path and each part of the trail is an active control. You can click on a folder name in the breadcrumb trail to navigate directly to that folder. You can also click an arrow for a folder in the breadcrumb trail to open a drop-down list of all subfolders within the folder. You can click a subfolder in the drop-down list to navigate directly to that location. |
| **Toolbar** | Contains buttons that enable you to perform tasks with files and folders in the contents pane. The tools change depending on the types of icons you select in the folder. |
| **Search box** | Search by name for an item within the current folder. |

| | |
|---|---|
| **Help** | Access Windows Help and Support options. |
| **Navigation pane** | You can click icons and folders in this pane to navigate the entire directory structure of the computer. |
| **Details pane** | Displays detailed information about the icon(s) or file selected in the Contents pane. |
| **Contents pane** | Displays the contents of the current folder. |
| **Preview pane** | When you select a file in the Contents pane, the Preview pane displays a preview of the file's contents when possible. If it cannot display a preview, it displays the text *No preview available*. |

You will use Windows Explorer periodically throughout the course.

# Configuring Desktop Settings

Objective 1.2

The Windows 7 user interface is completely configurable. That being said, it is important to keep in mind that many businesses elect to maintain a standard interface on all the systems throughout the organization. They may establish a particular color scheme, a particular set of icons and shortcuts on each Desktop, and configure the systems to disallow configuration changes from users.

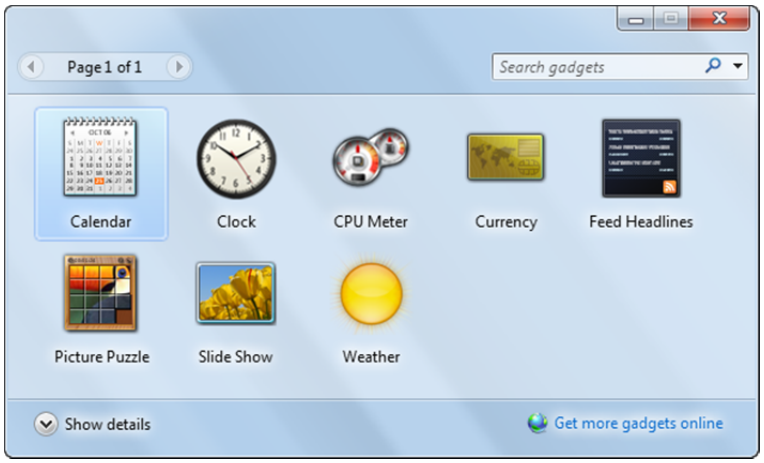
A uniform interface and configuration from one machine to the next can make it easier for users to work at any computer in the company, and can make it easier for the support staff to maintain and troubleshoot company systems. On the other hand, some companies allow for substantial "personalization" by standard users.

Regardless of the type of environment in which you find yourself, as an IT professional you should be comfortable configuring user desktops.

## Looking at Gadgets

Gadgets are mini programs that run on the Desktop instead of in an application window. Generally, they display information or perform a simple function. For example, a gadget can display the current date, while another can convert one currency into another.

Eight gadgets are installed in Windows 7 by default. These are: Calendar, Clock, CPU Meter, Currency, Feed Headlines, Picture Puzzle, Slide Show, and Weather. To view the installed gadgets, right-click a blank area of the Desktop, then click Gadgets to open the Gadget Gallery.




Double-click a gadget in the Gadget Gallery to add it to the Desktop.

You can easily install additional gadgets from the Microsoft Desktop Gadgets Web site. Click the Get more gadgets online link to access the Web site.

Most gadgets include configurable settings. You can right-click a gadget and then select Options from the shortcut menu. If Options is not available, then the gadget does not include configurable options. All gadgets include universal settings, such as the Always on Top setting and an Opacity (controls transparency) setting. Most gadgets can also be sized, and all of them can be repositioned anywhere on the Desktop.

Gadgets also include buttons which allow you to configure their appearance. You can point to a gadget to display its buttons. Gadget buttons can include a close button (which looks like an "x"; clicking it removes the gadget from the Desktop), a sizing button (which looks like an arrow; clicking it can increase or reduce the size of the gadget), an options button (which looks like a wrench; clicking it opens the Options menu), and a drag button (which looks like a grid; you can drag the gadget by its drag button).

## Exercise 2-1: Working with Desktop Gadgets

In this exercise, you will work with Desktop gadgets.

1. Right-click an empty area on the Desktop, then click **Gadgets** from the shortcut menu to open the Gadgets gallery.
2. In the Gadgets gallery, double-click **Calendar** to add the calendar gadget to the Desktop.
3. Point to the Calendar gadget on the Desktop to display its buttons. Click the **Larger size** button to enlarge the gadget.
4. Right-click the Calendar gadget, point to **Opacity** in the shortcut menu, then click **40%** to make the Calendar noticeably transparent.
5. Change the opacity back to 100%.
6. In the Gadgets gallery, double-click **Clock** to add the clock gadget to the Desktop.
7. Point to the Clock gadget on the Desktop, then click the **Options** button to access the configurable settings for the gadget.
8. In the Clock dialog box, click the **Next** (and Previous) buttons to page through the available clock faces until you find one that you like.
9. In the Clock dialog box, display the **Time zone** drop-down list, then select your time zone.
10. In the Clock dialog box, select the **Show the second hand** check box, then click **OK** to apply your changes.
11. In the Gadget gallery, click the **Get more gadgets online** link to open the Microsoft Desktop Gadgets Web page in your browser.
12. Scroll the Web page then click the **World Clock (37 Country Flag)** gadget, and specify to **Open** the file when prompted. In the Security Warning dialog box, click **Install** to add the gadget to the Gadget gallery and add it to the Desktop.
13. Close your Web browser.
14. Right-click the **World Clock (37 Country Flag)** gadget on the Desktop, then select **Options**. Scroll through the available country flags and select one for a country with which you might do business. Change the Time Zone to display the time for that region of the world. Set the remaining clock options to suit your personal taste, then click **OK**. Your Desktop may appear similar to the one shown below.


15. To remove a gadget from the Desktop, click its close button. On the Desktop, point to the **World Clock** gadget, then click its close button to remove it from the Desktop.

16. To remove a gadget from the gallery, uninstall it. In the Gadget gallery, right-click the **World Clock** gadget, then select **Uninstall**. Click the **Uninstall** button to confirm your selection and remove the gadget from the gallery.
17. On the Desktop, right-click the **Clock** gadget, then select **Close gadget** to remove it from the Desktop.
18. In the Gadget gallery, double-click **Slide Show** to add the slide show gadget to the Desktop, then close the Gadget gallery.
19. Enlarge the slide show gadget, then point to it and click on the **Next** button several times. The gadget should show a series of images; such as the eight default images in your Sample Pictures folder.
20. Remove the slide show gadget from the Desktop.
21. Consider how gadgets may be used and for what purposes. Which of the available gadgets on the Web site might be suitable for your business? Are there gadgets you might like to add to your home computer? Do you think office workers should be allowed to add gadgets to their office machines without restriction?

In this exercise, you worked with Desktop gadgets.

# Profiles

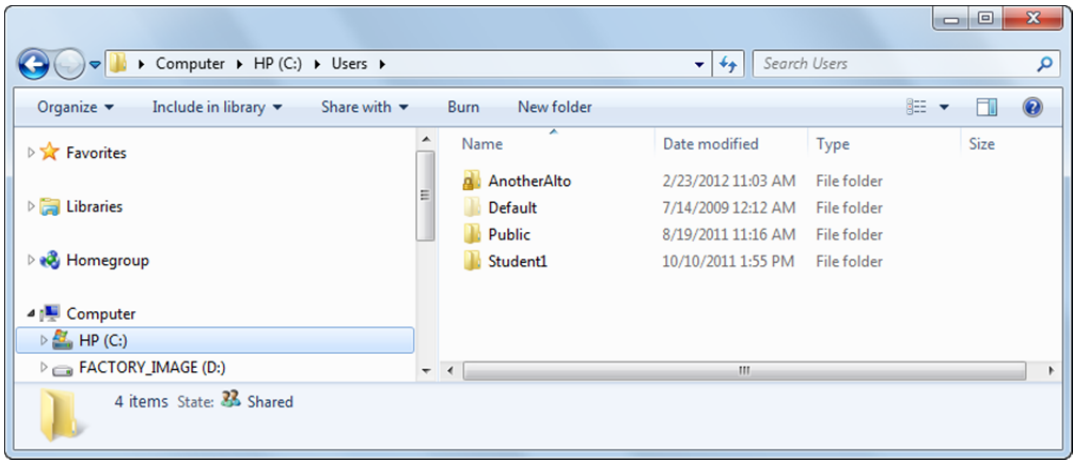
A user profile is a collection of settings that make the computer look and function in a particular manner. It is comprised of various Windows configuration settings for a specific user, including settings for Desktop background, screen saver, pointer preferences, network and printer connections, and mail settings. Whenever a user logs onto a machine, the settings in the associated user profile are loaded and affect what is displayed on the Windows Desktop and start menu.

A user profile is different from a user account. A user account is required to log on to Windows, and the settings associated with the user account control the user's rights on the system, such as which files and folders the user can access and what changes the user can make to the system. A user profile is part of a user account. (You will learn about user accounts in detail in a later lesson.)

Windows creates three specific profile types on the local machine:

| | |
|---|---|
| **Public profile** | Contains universal icons and items that should be available to all users. When you install an application and the installation wizard asks if you want to install the program for all users or only the current user, your answer determines which profile is updated. If you elect to make the program available to all users, the application settings and shortcuts are placed in the Public profile. Any shortcuts or files added to the Public profile are available to all user profiles on the machine – both existing ones and ones that will be created in the future. |
| **User profile** | Contains settings that are specific to an individual user. The user's preferences for window color, wallpaper, Desktop theme, screen magnification, etc., are saved to that user's profile. Documents that are placed on the Desktop are actually stored in a subfolder of the user's profile folder. When a user logs on to Windows, the condition and behavior of the Desktop are determined by settings in both the user's profile and the Public profile. |
| **Default profile** | The profile used by Windows as the boilerplate or template for creating new user profiles. If an enterprise elects to design and implement a standardized user profile, the system administrator can edit the default profile so that each new user profile will automatically include the standardized elements. This is accomplished with an answer file and customized system image. |

In Windows 7, user profiles are stored in the Users folder on the root of the system drive – typically drive C. The Users folder contains a single folder for each user profile. Each folder is named after the user. The Users folder also includes a folder for the Public profile and a folder for the Default profile. You can view the folders in Windows Explorer.



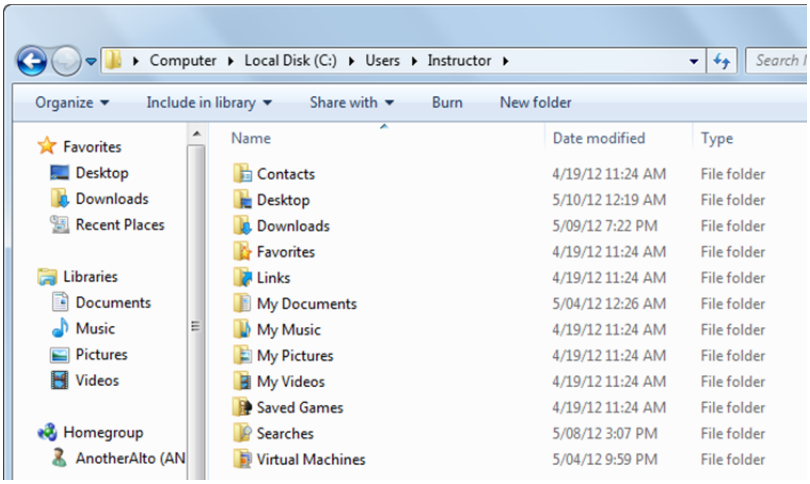

The Default folder is a hidden folder. To view hidden folders and files, you must specifically configure Windows Explorer to display them. You will learn how in the following exercise.

## Exercise 2-2: Accessing User Profile Folders

In this exercise, you will access the user profile folders.

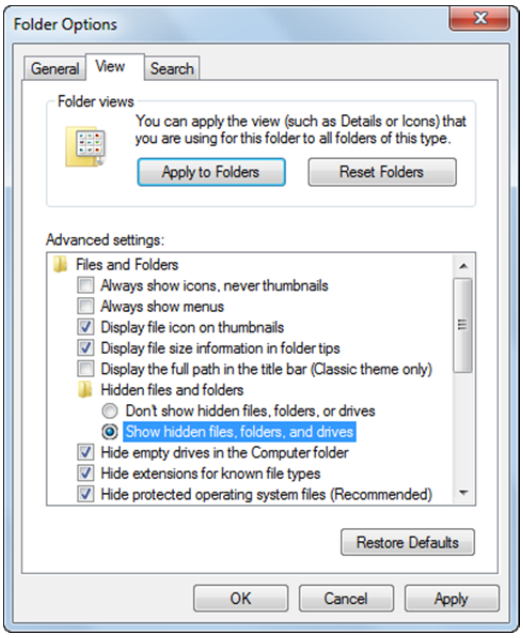
1. Right-click the **Start** button, then click **Open Windows Explorer** to open the Windows Explorer window.
2. In the navigation pane double-click **Computer** if necessary to open this tree and display all the local hard disk(s) underneath it.
3. In the navigation pane, click **Local Disk (C:)**. Note that your drive C: may be named something other than "Local Disk."
4. In the Contents pane, double-click the **Users** folder. You should see at least your profile and the Public profile.
5. In the Contents pane double-click your profile to view the subfolders inside.

   Each user profile includes the Contacts, Desktop, Downloads, Favorites, Links, My Documents, My Music, My Pictures, My Videos, Saved Games and Searches subfolders by default. Some profiles include additional folders. Your screen should appear similar to the one shown. You can double-click any of the subfolders to view their contents.




6. In the Contents pane double-click **My Pictures** to view the contents of the folder. Notice that the folder is empty.
7. In the address bar at the top of the Windows Explorer window, click **Users** in the breadcrumb trail to move back up through the directory structure.
8. In the Contents pane, double-click **Public** to access the public profile folder. Notice that the folders are similar to, but not exactly the same as, the ones in your personal profile.

9. In the Contents pane, double-click **Public Pictures**, then double-click **Sample Pictures** to view the image files that are available to all user profiles on the system. Notice that these are the eight image files that were displayed by the slide show gadget when you added it to your Desktop. Even though these image files are not saved in your user profile, programs running under your profile can access them because they are part of the Public profile.
10. In the address bar at the top of the Windows Explorer window, click **Users** in the breadcrumb trail to move back up through the directory structure.
11. In the Windows Explorer toolbar, click **Organize**, then click **Folder and search options** to open the Folder Options dialog box.
12. In the Folder Options dialog box, click the **View** tab, then under **Hidden files and folders**, select **Show hidden files, folders, and drives**.




13. In the Folder Options dialog box, click **Apply**, then click **OK** to apply the new settings. The previously hidden Default folder is now visible.
14. In the Contents pane, double-click **Default** to view the subfolders. Do not change any of the files in the Default folder.
15. Close the Windows Explorer window.

In this exercise, you viewed various user profile folders.

## Local Profiles and Roaming Profiles

When you create a user account on a computer, the user profile information is stored in the Users folder off the root directory of the system drive. This is referred to as a local profile; it is available only to the machine on which it is stored.

In organizations in which the company computers are part of a domain-based network, user accounts may be configured to use a roaming user profile instead. A roaming user profile allows users to log on to any computer within the same network and access their documents and have a consistent Desktop experience (Desktop appearance, sound scheme, screen magnification, applications, etc.) no matter which physical machine they log on to.

When a user account has a roaming profile, the profile information is stored on a centralized file server instead of on the local machine. This way, the user profile is accessible from any network-joined computer. When the user logs in, the local computer checks to see if the user can log in with a local account. If a local user account does not exist and the computer is joined to a domain, it will check (or authenticate) that account on that domain's Active Directory. If the domain login is successful, the roaming profile is copied from the central file server to the PC.

When the user logs off from the PC, the user's roaming profile is copied from the local machine back to the central file server. In this way, any changes made to the profile are saved at the central location.

# Changing Display Settings

Display settings include screen resolution, screen magnification and support for multiple monitors. Windows chooses optimal display settings based on the monitor. However, not every user is satisfied with the settings that Windows chooses. Some desire more screen space, while others prefer larger icons and text. In some cases, users can be more productive with a Desktop that extends across two (or more) monitors.

As an IT support professional, you should be able to adjust the display settings to suit the working style and needs of the employees. Display settings are accessed through various dialog boxes in the Control Panel.

## Adjusting Screen Resolution

Screen resolution refers to the degree of clarity with which text and images appear. Screen resolution is measured by the number of pixels (or dots) the screen can accommodate, and the measurements are given as width by height. For example, a resolution of 800 x 600 displays 800 pixels horizontally on the screen and 600 pixels vertically.

The resolution you can use depends on the resolutions your monitor supports. CRT monitors generally display a resolution of 800 × 600 or 1024 × 768 pixels and can work well at different resolutions. LCD monitors (flat-panel displays) and laptop screens often support higher resolutions and work best at their maximum resolution.

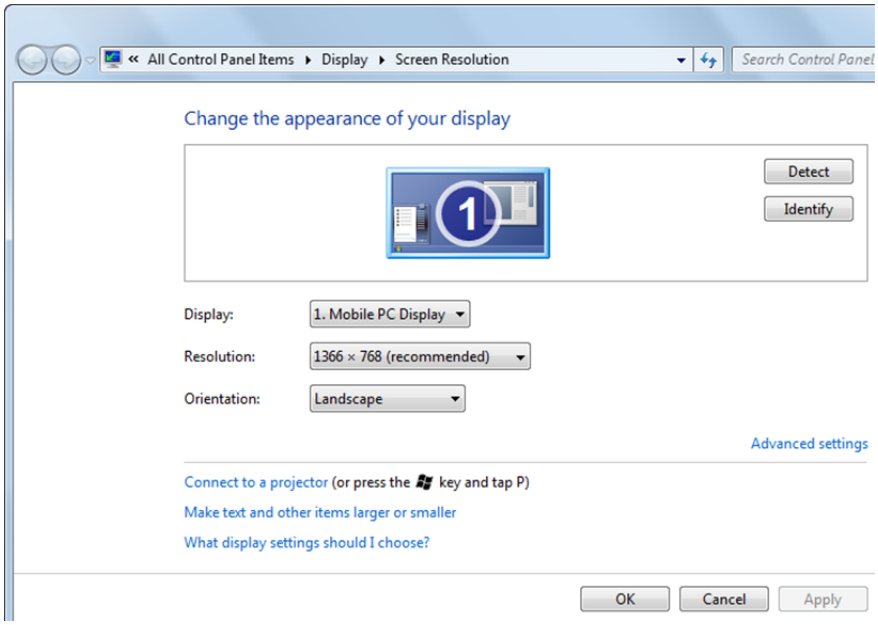
Regardless of whether you use a CRT or LCD monitor, you have the ability to adjust the display resolution. If you reduce the resolution (e.g. change from 1024 x 768 to 800 x 600), items displayed on the screen will appear bigger and their edges become more visible. Because the items are limited in how they are displayed, they become fuzzier (but if you move away from the monitor the items appear clearer again). The same effect occurs when zooming in on a low quality photograph – everything appears larger and grainier. This reduction in clarity is much worse with LCD monitors simply because of the limitation of the technology. As a result, everything displayed on a LCD monitor will be clearest when it is set to the highest resolution (also known as its native resolution). Therefore it is recommended that you set flat-panel monitors and laptop screens to their native resolution. The native resolution is identified in the Resolution drop-down list by the word *recommended*.

The larger the monitor, usually the higher the resolution it supports. Whether you can increase your screen resolution depends on the size and capability of your monitor and the type of video card you have.

Users may want (or need) to change the screen resolution for several reasons, including:

- An application requires a higher or lower resolution than the current setting.
- The user is unable to see the screen well at the current settings.

You can adjust resolution settings in the Screen Resolution dialog box.

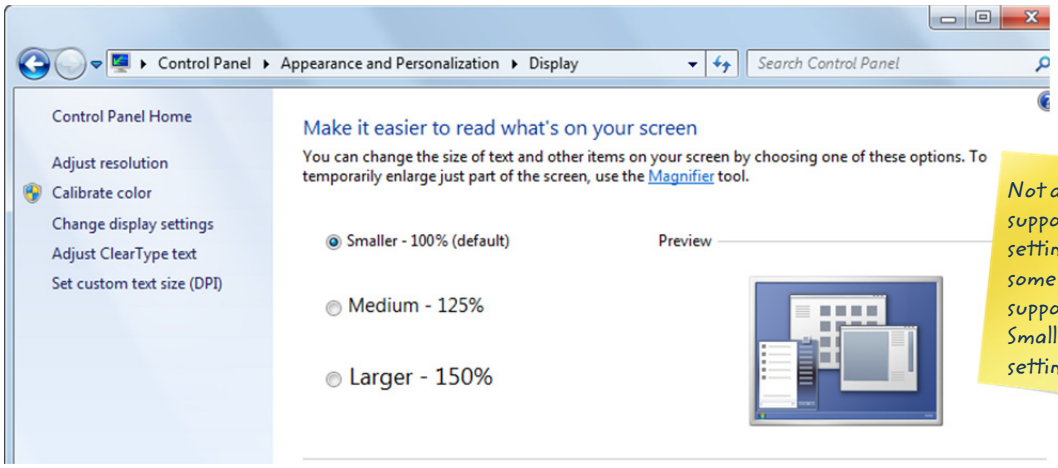



When you change the screen resolution, it affects all users who log on to the system.

## Adjusting Screen Magnification

It is also possible to adjust the size of text and other items on the screen without changing the screen resolution setting. There are three possible screen magnification settings – Smaller (100%), Medium (125%), and Larger (150%).

You can adjust magnification settings in the Display dialog box.




Not all monitors support all three settings. For example, some laptop screens support only the Smaller and Medium settings.

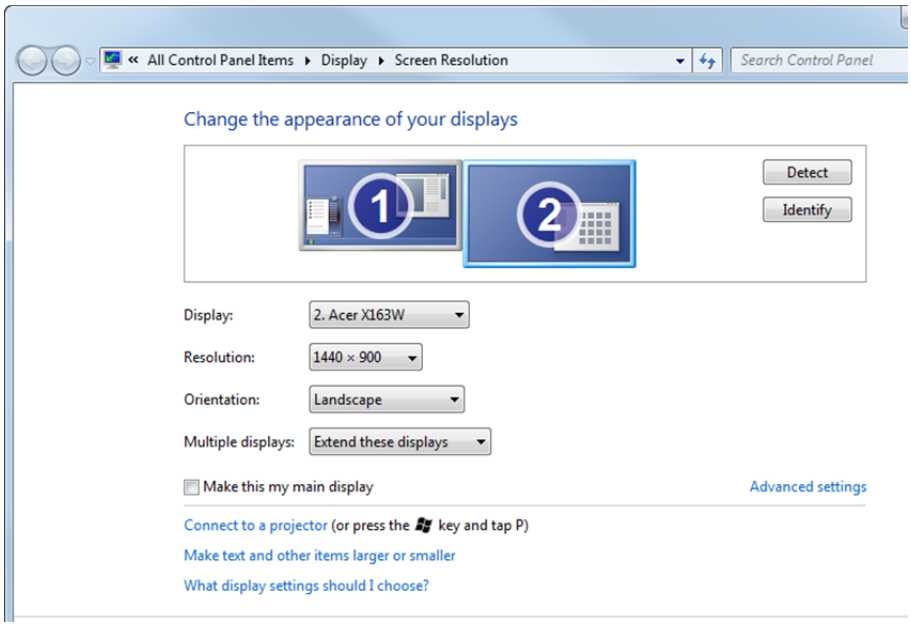
In addition to configuring the screen magnification, you can use the Magnifier tool to enlarge different parts of the screen. The Magnifier tool will be discussed in the accessibility options section later in this lesson.

## Configuring Windows to Support Multiple Display Devices

There are many situations in which a user may need to support multiple display devices. For example, you can connect a laptop to a projector and still use the internal screen. Or you can connect a Desktop or laptop computer to two monitors, enabling the user to view either identical output on both screens (duplicating the display), or extended output from one monitor to the other. The number of monitors that can be used is limited to the capabilities of the video card.

Extended displays can be ideal for significantly increasing the Desktop area because you can drag windows, program icons, and other items to any location on the extended Desktop. For example, a user might keep an e-mail open on one monitor, and work on documents or files on the other monitor. Or a user might view a different document or spreadsheet on each monitor and refer to one while working on the other, or drag information between them.

When multiple display devices are connected and detected, the Screen Resolution dialog box will show the different display devices and you can configure each one independently.



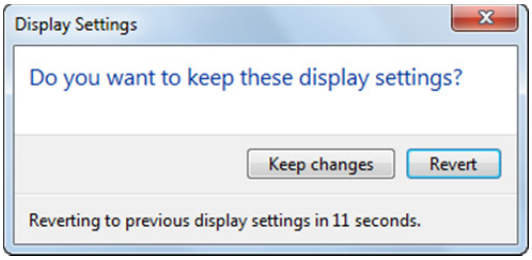
When you connect an external monitor or projector to a laptop, the same image of the Desktop appears on the external monitor by default. Before you can drag a window from the laptop screen to the external monitor, you must configure the external monitor as an extended display. In the Screen Resolution dialog box, display the **Multiple displays** drop-down list and select **Extend these displays**.

When you connect a second monitor to a Desktop PC, the display is set to "extended" by default and you should be able to drag a window from one screen to another without changing any settings.

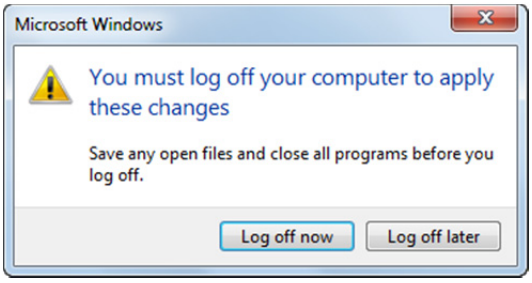
## Exercise 2-3: Adjusting Display Settings


In this exercise, you will adjust display settings.

1. Right-click a blank area of the Desktop, then click **Screen resolution** to open the Screen Resolution dialog box.
2. Display the **Resolution** drop-down list, drag the slider to the lowest setting, then click outside the drop-down list. An alert that some items may not fit on the screen may display.
3. Click **OK** to apply the new settings. A preview of the new setting appears. Notice how large the dialog box appears. You can elect to keep the new setting or revert to the previous setting. If you do not click the Keep changes button, Windows will automatically revert to the previous setting.




4. Click **Revert** to abandon the changes. Some of the icons on your Desktop may have moved to a different position as a result of your temporarily making the Desktop smaller. Also, any open application windows may now be smaller for the same reason.
5. If necessary, change the **Resolution** back to the original resolution (it should be the one marked ***recommended***).
6. In the Screen Resolution dialog box, click the **Make text and other items larger or smaller** link to open the Display dialog box.
7. Select an option that is not currently selected. An alert that some items may not fit on the screen may appear in the dialog box.
8. Click **Apply** to keep the new setting. Note that you must log off the computer in order to apply the changes. Unlike screen resolution settings, screen magnification settings are specific to individual user profiles.




9. Click **Log off now**.
10. Log back on and notice the change in appearance.
11. Change the magnification back to its previous setting, log off and log back on.

In this exercise, you adjusted display settings.

# Creating Shortcuts

A shortcut points to an executable file (i.e. a program), a document or a folder, and makes it possible to locate and open a file or launch a program with a single click. Without shortcuts, you would be required to browse through the files on the hard drive and locate the one you want each time you want to use it.

Shortcuts save time and allow users and support staff to work more efficiently. You can create shortcuts to programs, files or resources. For example, you can create a shortcut to a network printer that would allow you to view the current print queue or printer properties.

The shortcut itself is a small file that includes information on where the application, file or resource is located. You can configure properties that affect the appearance of the shortcut (such as its name or icon). You can also configure settings that are passed as parameters to the application being opened. For example, you can control the state of the window. In some cases, you can specify colors and other settings for the application itself.

## Creating Shortcuts for All Users

You also can create Start menu shortcuts that will be available to all users on the computer. To create a Start menu shortcut for all users, follow these steps:

1. Click **Start**, right-click **All Programs**, then select **Open All Users**.
2. Navigate to the application, right-click the application, then click **Pin to Start Menu**.

## Exercise 2-4: Working with Shortcuts

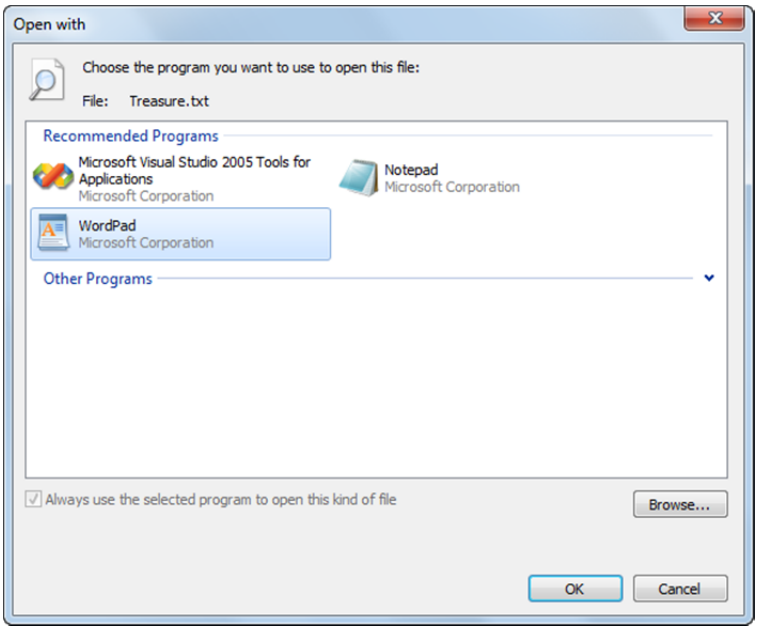

In this exercise, you will create, modify and delete shortcuts.

First, you will create a subfolder and a file, and create a Desktop shortcut to the file.

1. Right-click the **Start** button, then click **Open Windows Explorer**. You can also open Windows Explorer by clicking the **Start** button, then clicking **Computer**.
2. Double-click **Documents**, right-click in an empty space in the contents pane, point to **New**, then click **Folder**.
3. Type: `Buried`, then press ENTER.
4. Double-click the **Buried** folder, right-click in an empty space in the contents pane, point to **New**, then click **Text Document**, type: `Treasure`, then press ENTER.
5. Double-click the **Treasure** file to open it in Notepad.
6. Type: `This is my new file.` Press CTRL+S to save the file, then close the Notepad window.
7. Right-click the **Treasure** file, point to **Send to**, then click **Desktop (create shortcut)** to create a shortcut to the file on the Desktop.
8. Close the Windows Explorer window.
9. On the Desktop, double-click **Treasure** to open the file without having to navigate to it.
10. Close the Notepad window, then on the Desktop, right-click the **Treasure** shortcut, and select **Open file location**. A Windows Explorer window opens with the Treasure file selected. Notice in the Address bar that the file is still physically located in the Buried subfolder of the Documents folder. The file itself is not located on the Desktop.
11. Close the Windows Explorer window.

You can also modify the shortcut to specify that the file be opened with the WordPad application instead of with Notepad.

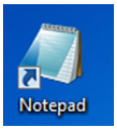
12. On the Desktop, right-click the **Treasure** shortcut, click **Properties** to open the Shortcut Properties dialog box, then click the **General** tab. Notice that the shortcut is currently configured to open the file with Notepad.
13. Click the **Change** button, select **WordPad** in the Open With dialog box.



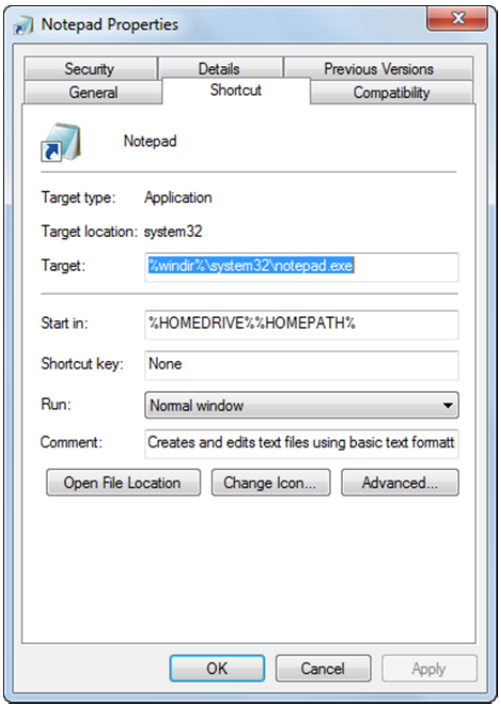

14. Click **OK** to apply the new setting. The shortcut is now configured to open the file using WordPad.
15. Click **OK** to close the Shortcut Properties dialog box.
16. On the Desktop, double-click the **Treasure** shortcut. This time the file opens in WordPad.
17. Close the WordPad window.

Next, you will create and modify a Desktop shortcut to the Notepad application.

18. Click the **Start** button, point to **All Programs**, click **Accessories**, locate the Notepad application, right-click **Notepad**, point to **Send to**, then click **Desktop (create shortcut)** to create a shortcut on the Desktop.
19. Click anywhere outside the Start menu to close the menu and view the newly created shortcut icon.




20. Double-click **Notepad** on the Desktop to test the shortcut, then close the program.
21. On the Desktop, right-click **Notepad** and browse the options in the shortcut menu. Notice that you can pin the shortcut to the Taskbar and/or to the Start Menu.
22. In the shortcut menu, click **Properties** to open the Notepad Properties dialog box. You can use the dialog box to configure how the shortcut will appear and behave. The available options depend on the application. The contents of the Target box show the path to the Notepad application.



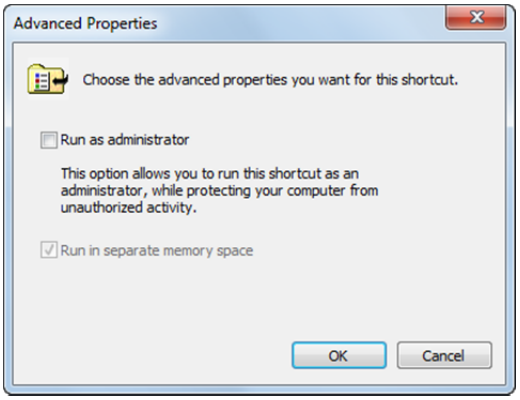

23. Display the **Run** drop-down list. You can configure the shortcut to open the application in a normal (restored) window, a minimized window (i.e., a button on the Taskbar), or a maximized window. Select **Minimized**, then click **OK**.
24. On the Desktop, double-click **Notepad** to open the application in a minimized state.
25. Click the **Notepad** icon in the Taskbar to restore the window.
26. Close the Notepad application.
27. On the Desktop, right-click **Notepad**, select **Rename**, type: `Text Editor` and press ENTER to rename the shortcut.


Next, you will create a Desktop shortcut to the Command Prompt application, and set parameters that control the application's appearance.

28. Click the **Start** button, point to **All Programs**, click **Accessories**, locate Command Prompt, right-click **Command Prompt**, point to **Send to**, then click **Desktop (create shortcut)** to create a shortcut on the Desktop.
29. Click anywhere outside the Start menu to close it.
30. On the Desktop, right-click **Command Prompt**, then click **Properties**. Notice that the Properties dialog box for the command prompt shortcut contains more tabs that the one for Notepad.
31. Click the **Layout** tab, then in the Window size area, change the Width setting to **100** and the Height setting to **45**.
32. Click the **Colors** tab. Ensure that Screen background is selected, then click the **navy blue** square to set the screen background to blue.
33. Click **OK** to save the changes, then double-click the **Command Prompt** shortcut to open a blue command prompt window.
34. Close the Command Prompt window.

You can also add administrator requirements to a shortcut; that is, you can require that only an administrator or a user who can supply administrative credentials can use the shortcut.

35. Right-click the **Command Prompt** shortcut, then select **Run as administrator**. Notice that the User Control Agent asks for confirmation that you want to allow the program to make changes to the computer. (If you were logged on as a standard user, you would be prompted to supply the user name and password of an administrator account.)
36. Click **No**.
37. Display the properties for the Command Prompt shortcut, click the **Shortcut** tab if necessary, then click the **Advanced** button, to open the Advanced Properties dialog box.




38. Select **Run as administrator**, then click **OK**.
39. Click **OK** once more.
40. On the Desktop, double-click the **Command Prompt** shortcut. This time the User Account Control agent appears because the shortcut automatically specifies to run the program as an Administrator.
41. Enter the password for the administrator account if necessary and click **Yes** to open the command prompt window. Notice that Administrator: Command Prompt displays in the title bar.
42. Close the Command Prompt window.
43. On the Desktop, right-click the **Text Editor** shortcut, select **Delete**, then click **Yes**.
44. On the Desktop, click the **Command Prompt** shortcut, press the **DELETE** key, then click **Yes**.
45. Delete the Treasure shortcut.

Finally, you will create a Start menu shortcut.

46. Click the **Start** button, point to **All Programs**, click **Accessories**, locate Paint, right-click **Paint**, then click **Pin to Start Menu**.
47. Click anywhere outside the Start menu to close it.
48. Click the **Start** button. Notice that Paint now appears at the top of the Start menu.
49. In the Start menu, click **Paint** to open the application.
50. Close the Paint window.

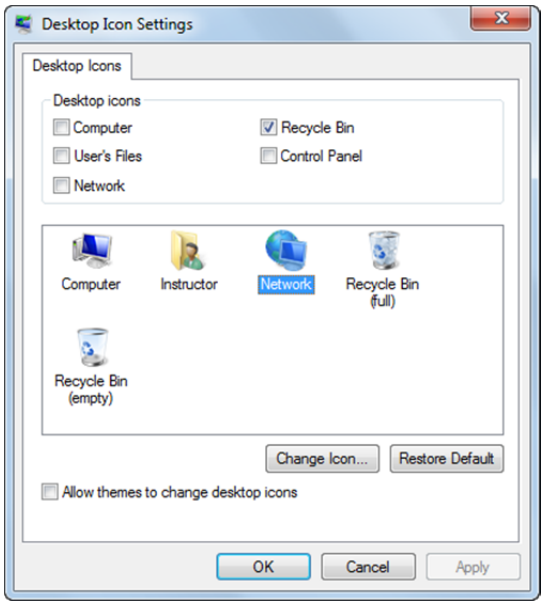
In this exercise, you worked with shortcuts.

## Adding System Icons to the Desktop

By default, the only system icon added to the Desktop is the Recycle Bin. A system icon is a special shortcut that launches a system component. System icons are built in to Windows. System icons include:

- Computer – shows the drives and other hardware connected to the computer
- User's files – shows the user profile folder
- Network – shows the systems and devices in the local network
- Recycle Bin – opens the Recycle Bin
- Control Panel – opens the Control Panel

System icons are easily identified because they do not contain a blue arrow in the lower-left corner by default. System icons are managed in the Desktop Icons Settings dialog box.




To add or remove system icons to the Desktop:

1. Right-click an open area of the Desktop, then click Personalize.
2. Click the Change Desktop Icons link in the left panel to open the Desktop Icon Settings dialog box.
3. In the dialog box, select or clear the check boxes as appropriate to indicate which icons you want to display on the Desktop, then click OK.

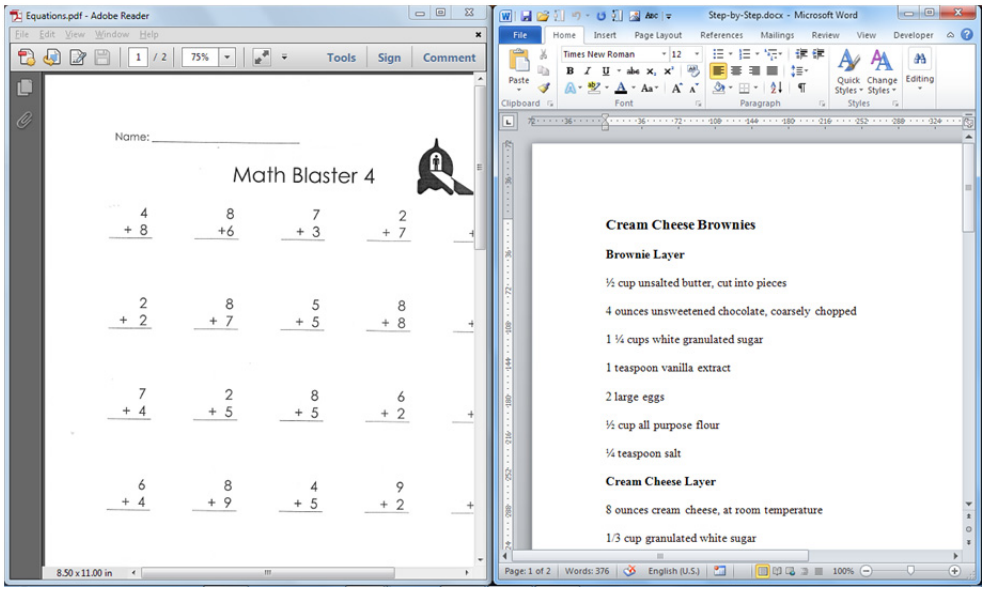
After adding the icons to the Desktop, you can quickly access them to browse files, manage the Recycle Bin, or access Control Panel. You can also use them for quick access to administrative tools. For example, you can right-click the Computer icon on the Desktop and select Properties to view the Control Panel System page.

## Working with Aero

The Aero interface allows for many advanced Windows management features. These features include:

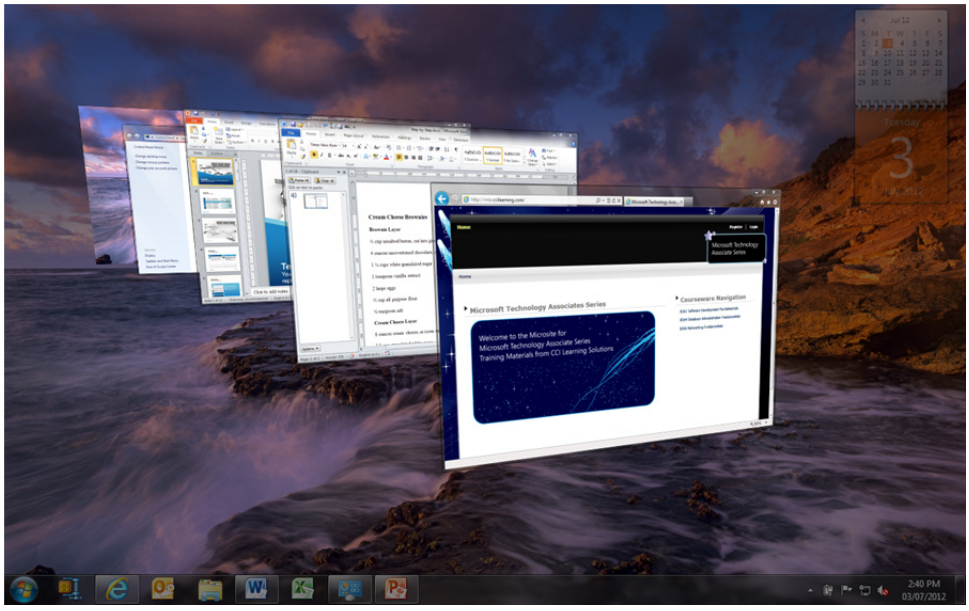
**Aero Snap**

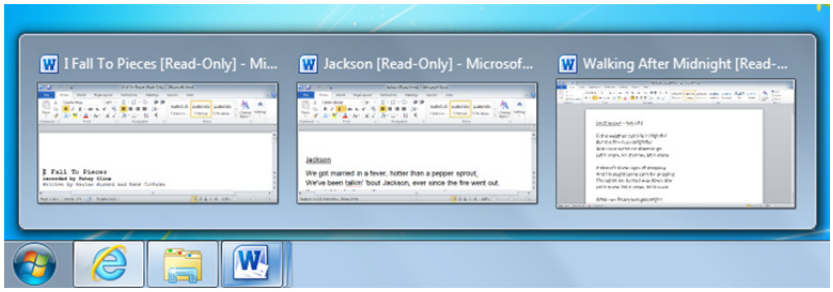
Allows you to view two windows side by side without having to manually resize them. Simply drag a window to the left or right edge of the Desktop and it will resize automatically.




**Aero Shake**

If you have several windows open, you can click the title bar of one window and then jiggle the mouse back and forth to minimize all other windows. Perform the action again, and the other windows return to their previous states.

| | |
|---|---|
| **Aero Peek** | Allows you to temporarily make all open windows transparent so you can see the Desktop. You can point to the Show Desktop button at the right edge of the Taskbar to peek at the Desktop. Once you move the mouse pointer away from the Show Desktop button, the open windows reappear. You can also click the Show Desktop button to minimize all open windows at once so that you can access the Desktop. Click the button again to restore all windows to their previous size and position.   |
| **Flip 3D** | Allows you to arrange your open windows in the 3-dimensional stack that you can quickly flip through without having to click the Taskbar. Press and hold WINDOWS+TAB to flip through the open windows in a continuous motion, or press and hold WINDOWS then press TAB once to open the view, then press TAB to advance through the windows one window at a time.  |

| | |
|---|---|
| **Taskbar Previews** | Allows you to see thumbnail previews of the windows. Thumbnails show running video, you can play and pause video and songs in a thumbnail, and close the windows without restoring them. If you point to a thumbnail, you can see a full-sized preview of the window. Click a thumbnail to access the window.<br>  |
| **Translucent windows** | Aero themes use transparent (or partially transparent) window frames, which allows you to see through the title bars to the application windows and objects behind the window currently on top.<br>  |
| **Improved window switching** | When you press ALT+TAB to switch between open windows, you can see live previews of the windows for each open program instead of just a program icon.<br>  |

To use the Aero features, your system must meet the following hardware requirements:

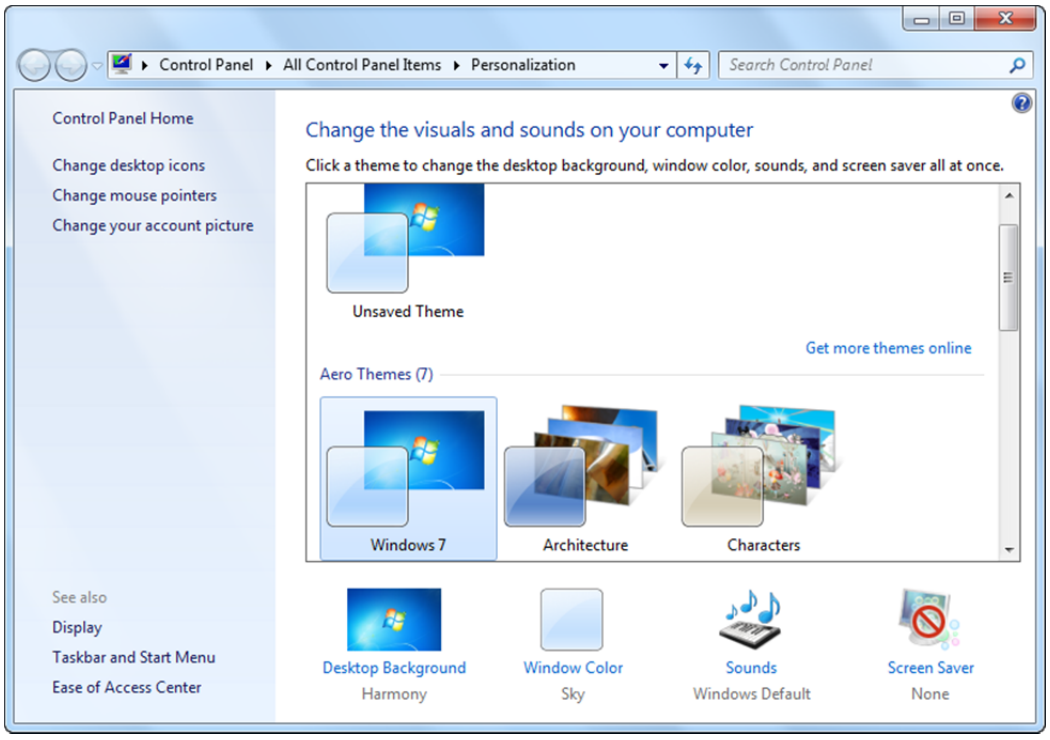
- 64 MB of graphics memory for resolutions up to 1280×1024
- 128 MB of graphics memory for resolutions higher than 1280×1024 and up to 1600×1200
- 256 MB of graphics memory for resolutions higher than 1600×1200

Additionally, you must use an Aero theme and you must have the Aero settings enabled.

## Aero Themes

Aero themes are Windows 7 themes that include support for Aero features. The two primary types of themes available in Windows 7 are Aero themes and basic themes. Basic themes do not support Aero features. Windows 7 comes with seven Aero themes, and you can get additional themes online.

A theme is a combination of pictures, colors and sounds. Each theme includes a Desktop background, a window border color, sounds and a screensaver. Right-click an open area of the Desktop, then click Personalize to open the Personalization window of the Control Panel.



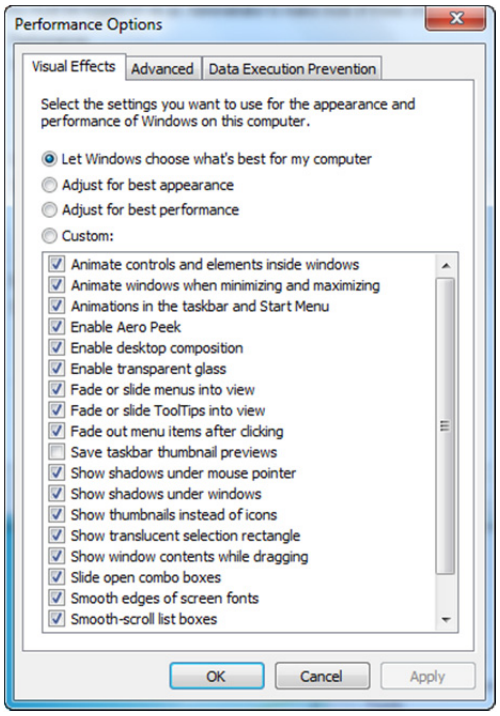

There are four types of themes:

| | |
|---|---|
| **My Themes** | These are themes you have customized, saved or downloaded. When you make changes to a theme, the new settings appear in this section as an unsaved theme. |
| **Aero Themes** | These themes include Aero glass effects and many include a desktop background slide show. |
| **Installed Themes** | These are themes that are created by computer manufacturers or non-Microsoft providers. Not every system includes installed themes. |
| **Basic and High Contrast Themes** | These themes are designed to improve computer performance or to make items easier to see. These themes do not include Aero glass effects and therefore do not support all of the Aero features. |

Click any theme in the dialog box to select it. For the selected theme, you can change the window color, sounds and screen saver settings. Simply click the theme component at the bottom of the Personalization window to access the configuration settings.

Supporting the Aero features can impact the performance of the system, especially if the system only barely meets the hardware requirements.

You can adjust which features are supported by enabling or disabling the individual features of an Aero theme in the Performance Options dialog box. To open this dialog box, click the **Start** button, right-click **Computer**, then click **Properties**. Click the **Advanced system settings** link in the left panel of the System window, click the **Advanced** tab if necessary, in the Performance area click the **Settings** button to open the Performance Options dialog box and click the **Visual Effects** tab if necessary.

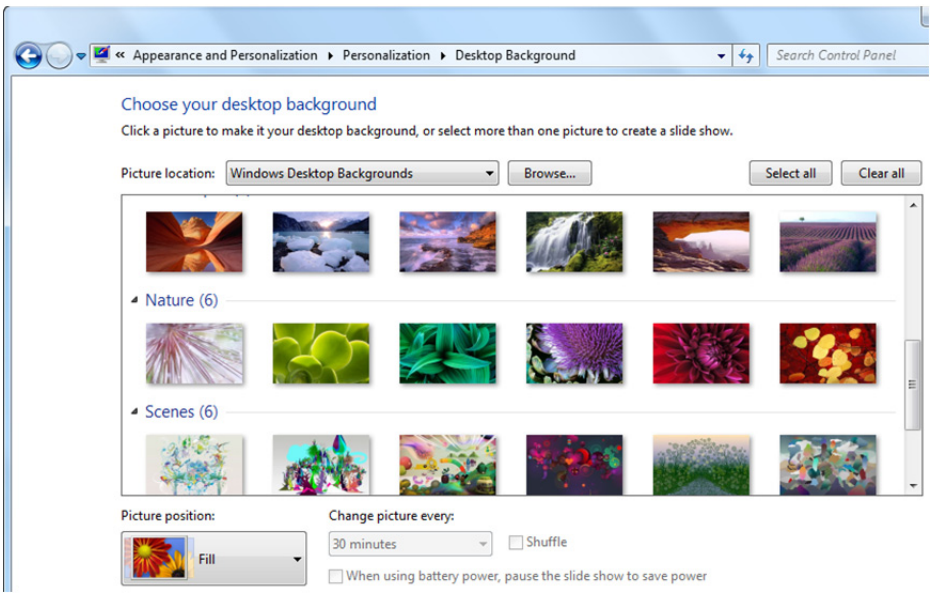



You can also select one of the options at the top of the dialog box – Let Windows choose what is best for my computer, Adjust for best appearance, Adjust for best performance, or Custom. Once you begin clearing or selecting check boxes, the Custom option is selected automatically. You can return to the original settings by specifying to allow Windows to choose.

## Exercise 2-5: Modifying an Aero Theme

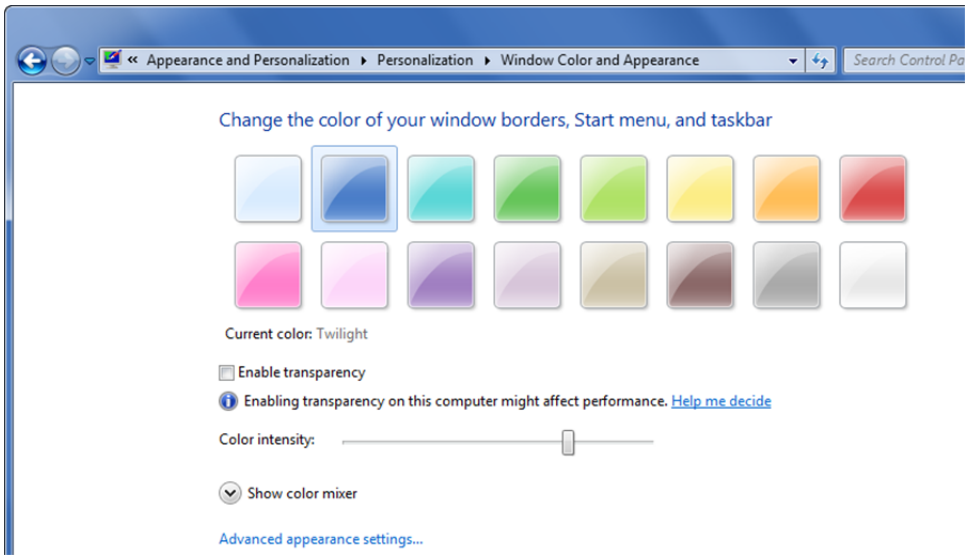
In this exercise, you will work with Desktop theme settings.

1. Right-click an empty area on the Desktop, then click **Personalize**.
2. In the Themes area of the window, click **Windows 7** under Aero Themes.
3. Below the Themes area, click **Desktop Background** to access the Desktop Background window.



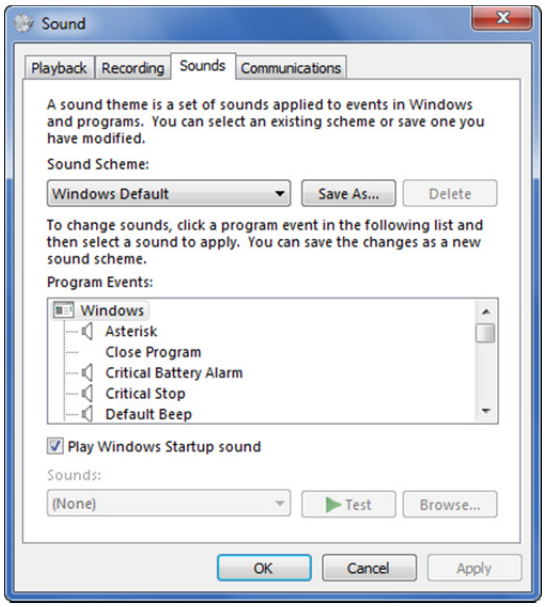
4. Click the background of your choice, then click **Save changes** to specify a Desktop background and return to the Personalization window.

5. Below the Themes area, click **Window Color** to access the Window Color and Appearance window. Here you can select a color for the windows borders, the Start menu and taskbar. You can also specify whether to enable transparency, and you can set the color intensity. On some systems, enabling transparency can put a strain on system resources.



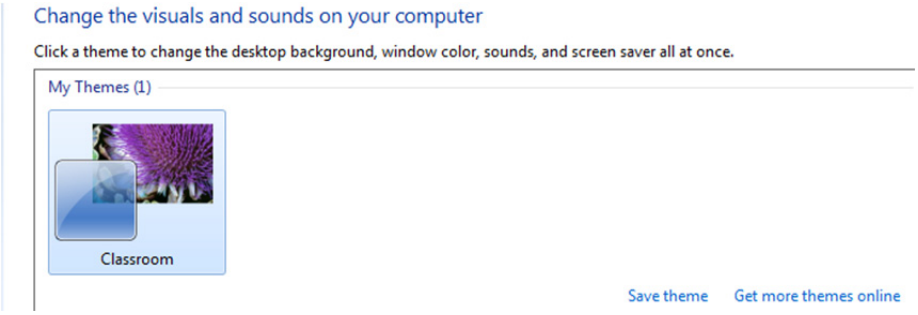

6. Click one of the colors to select it, then either select or clear the Enable transparency check box according to your preference. Note that disabling transparency does not affect the function of the Aero features. When you have made your selections, click **Save changes** to apply your color settings and return to the Personalization window.

7. Below the Themes area, click **Sounds** to open the Sound dialog box. The sound settings for specific program events are grouped into named sound schemes. You can customize a Windows theme by specifying any sound scheme you like. You can also change individual sounds within the sound scheme.




8. Display the Sound Scheme drop-down list, select **Garden**, then click **OK** to save the settings. Your modifications are currently saved to the Unsaved Theme in the My Themes section of the window.

9. Click the **Save theme** link to open the Save Theme As dialog box. Type: `Classroom`, then click **Save**. Your named theme appears in the My Themes section of the window.




10. In the Aero Themes section, click **Windows 7** to apply the built-in theme. Notice the immediate change on the Desktop behind the open dialog box. You should also hear the Windows Change Theme sound specified in the Windows Default sound scheme.
11. In the My Themes section, click **Classroom** to apply your customized theme. You hear the Windows Change Theme sound specified in the Garden sound scheme.
12. Keep whichever theme you prefer, then close the Personalization window.

In this exercise, you modified the settings for a Windows 7 Aero theme.

# Understanding Native Applications and Tools

Objective 1.3

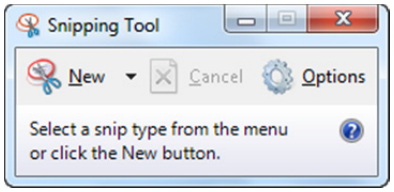
Native applications and tools are those that are built into Windows 7. Some of these are familiar utilities and applications such as Calculator, Notepad, WordPad and Paint. Most users are familiar with these tools from earlier Windows versions of the operating system and do not require extensive assistance using them.

On the other hand, users may feel overwhelmed by newer features, or those with extensively configurable interfaces. You should be able to demonstrate to users how to use the Snipping tool, and should be familiar with the major features of Internet Explorer, Windows Media Player and the Windows Media Center in order to provide assistance or help users work comfortably and efficiently.

Additionally, you should understand the MSCONFIG tool, which is a utility you can use to view and manage various configuration settings.

## Snipping Tool

You can use the Snipping Tool to capture a screen shot (called a snip) of any object on the screen. You can capture an area of the screen, a window or dialog box, or you can capture the entire screen. Once the snip is captured, you can annotate it, save it and even send it in an e-mail message.




You can save the captured image in the following formats:

- Portable Network Graphics (PNG)
- Graphics Interchange Format (GIF)
- Joint Photographic Experts Group (JPEG)
- Single file HTML (MHT)

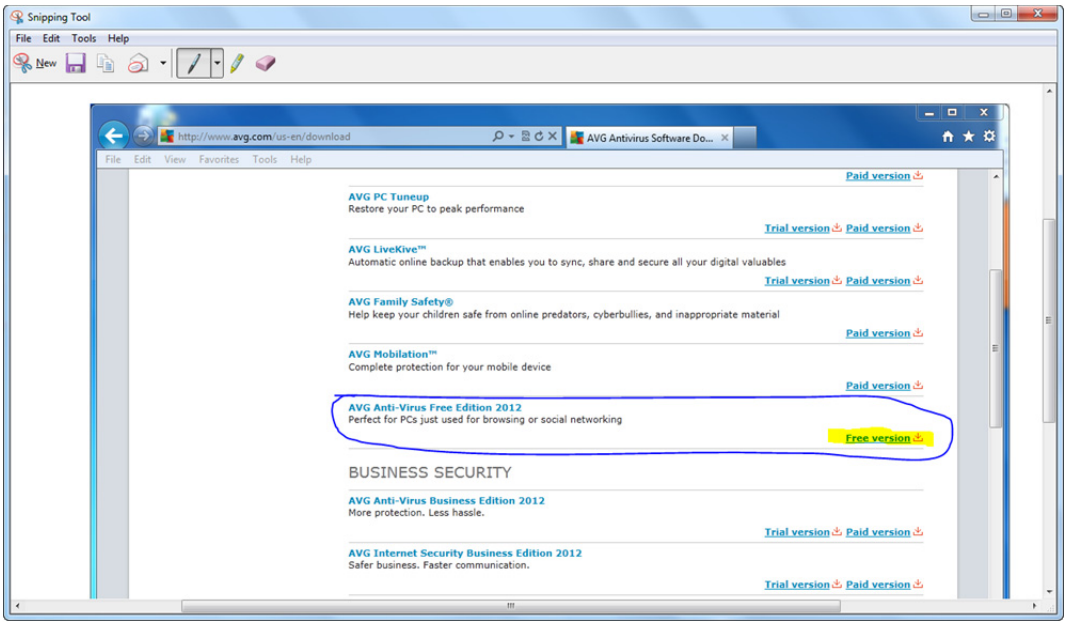
When you capture an image from a browser window, the suggested file format is MHT.

The snipping tool is easy to use and can be a useful tool in the trouble-shooting process. For example, a user can capture a screen shot of an error message and e-mail it to the support staff. If an IT person cannot provide on-site help (for example, the user is a remote employee), he or she can send an e-mail message that includes an annotated snip highlighting particular settings that should be used.

## Exercise 2-6: Using the Snipping Tool

In this exercise, you will use the snipping tool. Suppose you are trying to show a user where she can obtain the free version of a popular antivirus program to install on her home computer. You can get a screen capture and use the Pen and Highlight tools to show her exactly where to find the necessary links on the Web site.

1. Click the **Start** button, click **All Programs**, click **Accessories**, then click **Snipping Tool** to start the application. The windows Desktop is dimmed and the Snipping Tool is in the foreground.
2. Press Esc to access the Desktop.
3. Open your browser and go to the AVG Software Download page at **www.avg.com/us-en/download**. If the window is maximized, restore it and resize it so you can see a reasonable amount of the Web page.
4. Scroll down until the AVG Anti-Virus Free Edition 2012 download link is visible.
5. In the Taskbar, click the **Snipping Tool** button to access the tool.
6. In the Snipping Tool toolbar, click the drop-down arrow to the right of the New button, then select **Window Snip**. A red frame appears around the browser window.
7. Click anywhere in the browser window to capture the screen. The image displays in the Snipping Tool editor.
8. In the Snipping Tool toolbar, click the **Highlighter** tool, then drag the cursor over the Free Version link in the image.
9. In the Snipping Tool toolbar, click the **Pen** tool, then circle the AVG Free option on the image, as shown below:




10. In the Snipping Tool toolbar, click the drop-down arrow to the right of the Send Snip button to view the options for sending the snip in an e-mail message. You can send the image in-line with the message text if the file format is MHT and if the e-mail client creates messages in HTML format. You can also specify to send the image as an attachment to the e-mail message.
11. Click in a blank area of the Snipping Tool window, then in the Snipping Tool toolbar click the **Save Snip** button to open the Save As dialog box.
12. In the Navigation pane, click **Desktop**, type: `FreeLinks` as the file name, display the Save as type drop-down list, then select **Portable Network Graphics file (PNG)**, then click **Save**.
13. Close the Snipping Tool and close the browser.
14. On the Desktop, double-click the *FreeLinks* file to open in it Windows Photo Viewer to see that it is a standard image file.
15. Close Windows Photo Viewer.

In this exercise, you used the Snipping Tool.

# Windows Internet Explorer

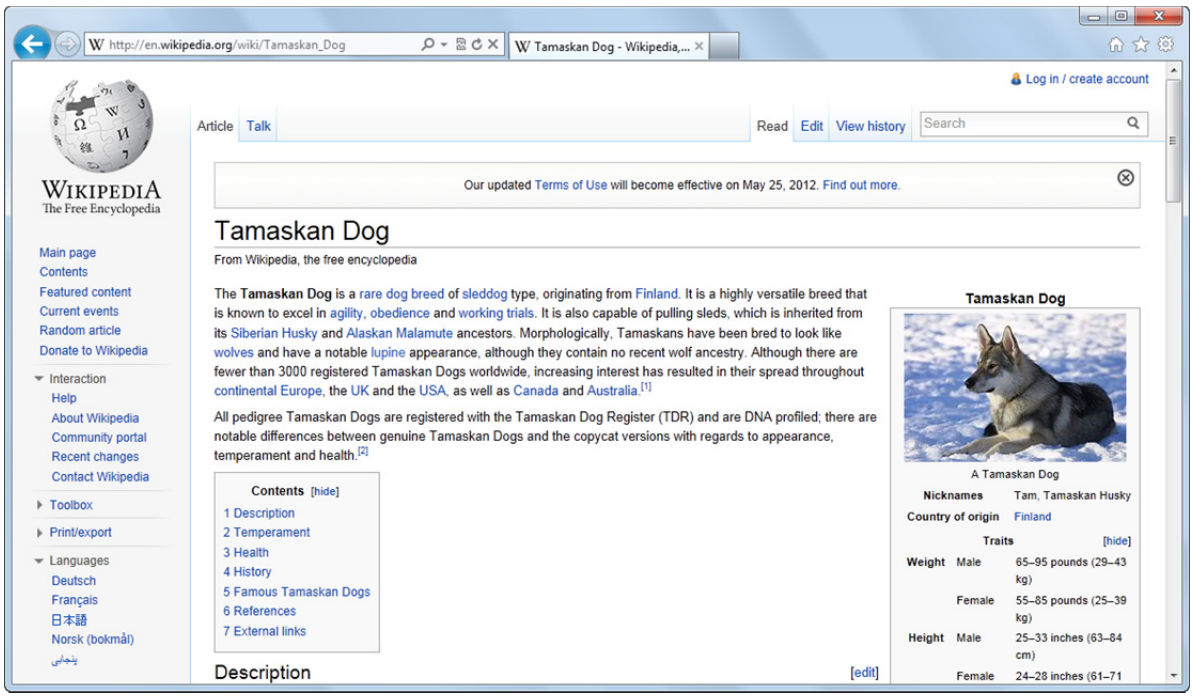
Objective 1.3

A Web browser's primary function is to retrieve pages from a Web server and display those pages on the screen. Millions of people use browsers every day for research, shopping, entertainment, etc. While just about anybody can open a browser and browse the Web, an IT professional can understand the processes at work, identify and avoid potential risks, and configure a browser to suit the working styles of employees and conform to any corporate standards.

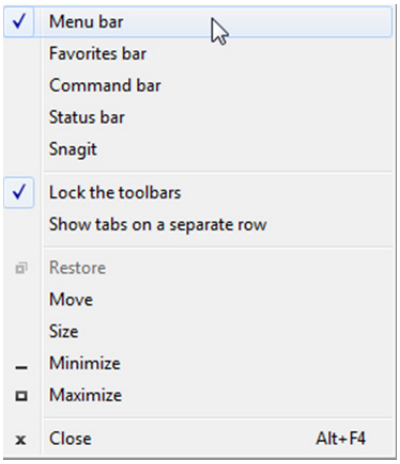
*Windows 7 comes with Internet Explorer 8.0 installed, but Internet Explorer 9 is the current standard. If a system is configured to download and install automatic updates, it will be updated to Internet Explorer 9.*

## Streamlined Interface

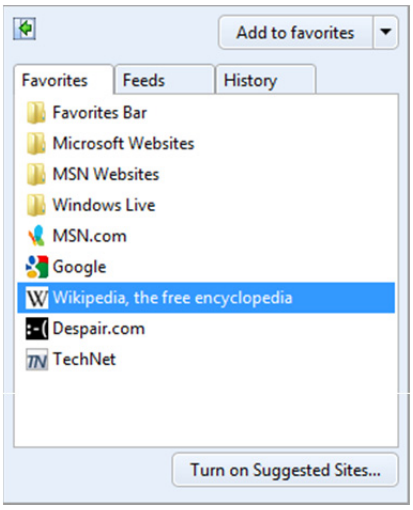
As with any "new and improved" version of software, certain new features or revised layouts can cause confusion among users. Internet Explorer 9 has a stream-lined appearance; the Favorites bar, menu bar, command bar and status bar are turned off by default, as shown in the following figure:




Users can display these familiar tools by right-clicking an empty area of the title bar, then selecting the items they want to show.



You can also view Favorites by clicking the Favorites button at the right edge of the window to open the Favorites center, which can be resized, or moved to the left edge of the window.




# Useful Tools and Features

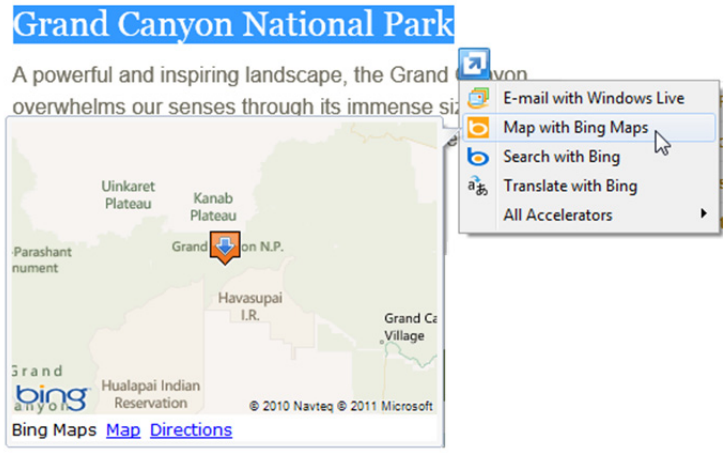
The following tools and features can help individuals work more efficiently and more securely. You may have occasion to demonstrate these tools and features to employees within your organization.

## Accelerators

An accelerator allows you to start an online service from another Web page without navigating away from the current page. You can select text or other objects to access the usable accelerator services (such as opening a blog, or viewing a map to a selected location.) The purpose of an accelerator is to eliminate the need to copy and paste content between Web pages.

For example, if a corporate team-building event were scheduled to take place at Grand Canyon National Park in Arizona, you could select the text Grand Canyon National Park and an accelerator button would automatically appear, as shown.


Click the accelerator button to view the available accelerators, and then click one to launch it.

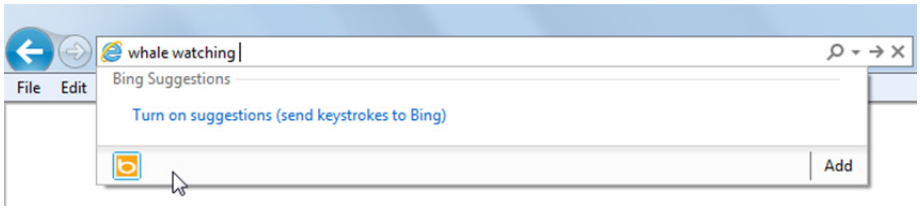



Accelerators are add-ons – small programs that add features such as extra toolbars, stock tickers, etc., to the Web browser. Add-ons are often provided by a third party vendor. The default accelerators built in to Internet Explorer 9 are: E-mail with Windows Live, Map with Bing, Search with Bing, and Translate with Bing. You can add more from the Internet Explorer Gallery at www.iegallery.com.

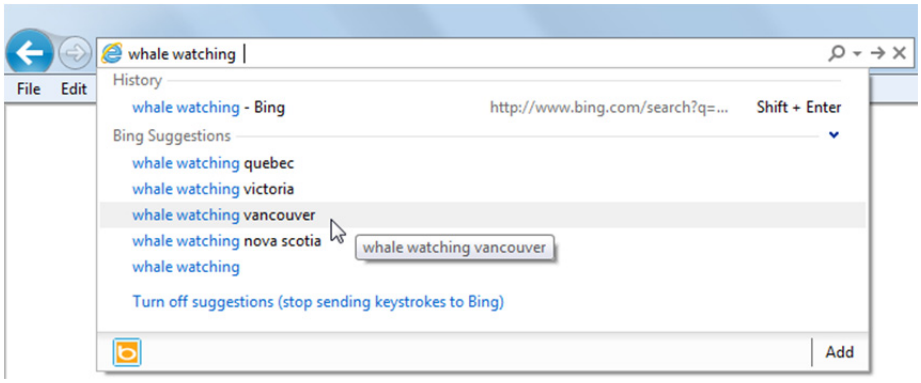
To manage add-ons (including disabling or removing them), click the **Tools** button, then click **Manage add-ons**.

## Searching from the Address Bar

You can now search directly from the Address bar instead of first accessing a search engine page. Simply click in the Address bar and start typing. If you enter a complete URL, you will go directly to the Web site. If you enter a search term or an incomplete address, click a search provider in the menu to launch a search using the currently selected search engine.




You can also click **Turn on suggestions** to display a list of suggested search terms.

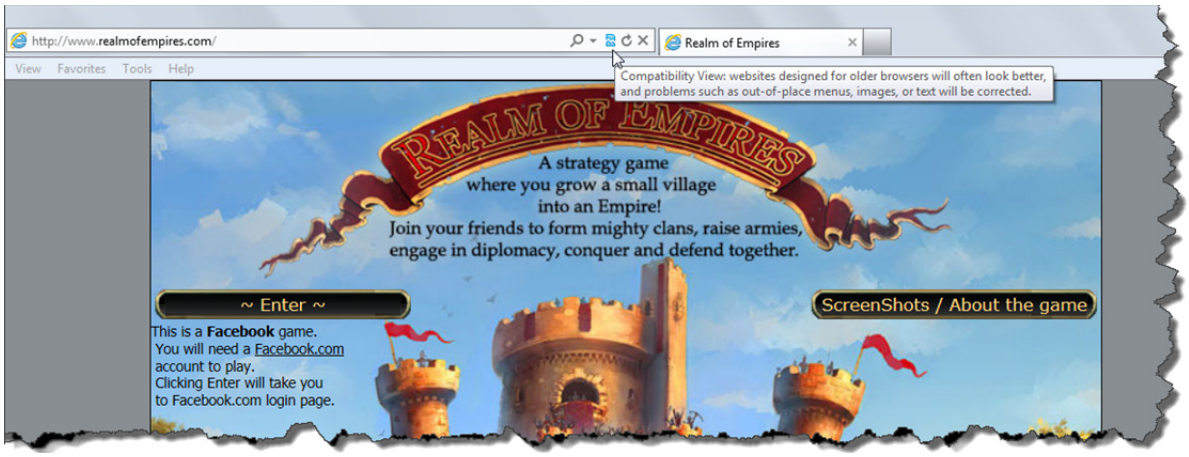



You can also click the **Add** button in the drop-down menu to add search providers (such as Google or Ask.com) from the Internet Explorer Gallery Web site.

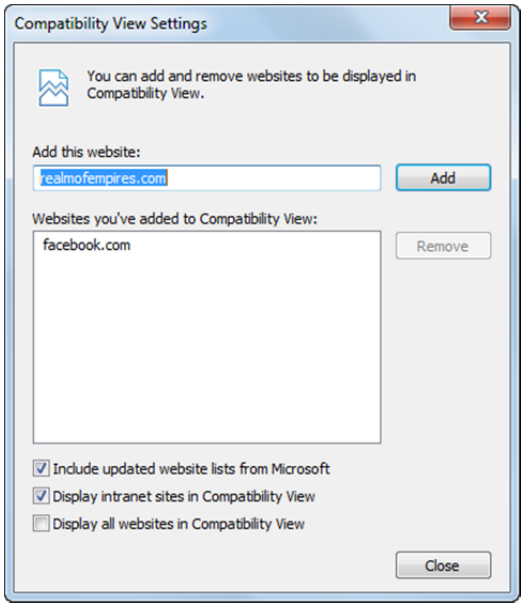
## Compatibility View

Certain older Web sites that were designed for earlier versions of the Internet Explorer Web browser may not display correctly in Internet Explorer 9. (For example, they use deprecated tags or rely on server extensions that are no longer supported.) This can often be the case with sites designed for a corporate intranet, or sites on a corporate partner's extranet.

You can force these pages to display correctly using Compatibility view. In most cases, Internet Explorer will detect a compatibility problem with a particular Web site and will automatically display the Compatibility View button in the Address bar.



Click the **Compatibility View** button to display the site in Compatibility View. Click it again to disable Compatibility View. To specify that a particular Web site should always display in Compatibility View, navigate to the site, then in the Internet Explorer menu bar, click **Tools**, then click **Compatibility View Settings** to open the Compatibility View Settings dialog box. Click the **Add** button to add the site to the list box, then click the **Close** button.




Notice that by default, intranet sites are set to display in Compatibility View.

In some organizations, it may be the standard to configure the browser to set all Web sites to display in Compatibility View. If a website doesn't display correctly, you can turn off Compatibility View by clicking the Compatibility View button.

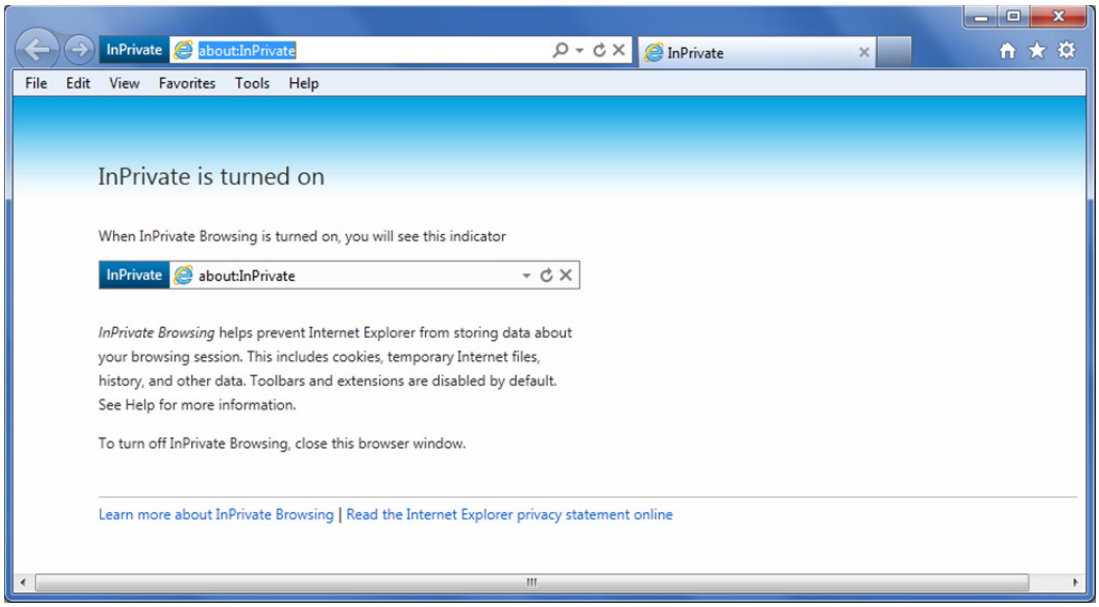
## InPrivate Browsing

The InPrivate Browsing feature enables anonymous browsing. That is, users can use the browser and leave no evidence on the hard drive of the sites or content they have browsed.

As you browse the Web, the History folder stores the URLs of sites you have accessed within a defined period of time, and provides a convenient way to revisit Web sites, especially if you cannot remember the exact URL. In Internet Explorer, the default amount of time to keep pages in History is 20 days.

Additionally, as you surf, content is copied to the browser cache. The browser cache is a folder on your hard drive that stores downloaded files (such as Web pages, images, fonts, etc.). The cache improves your browser's performance because it allows you to view previously accessed Web pages without having to request them from the server again. For example, if you click a hyperlink on a Web page, then click the browser's Back button, the browser can pull the previously viewed page from the cache.

When a user opens an InPrivate browsing session, a new window opens. The window is clearly identified as an InPrivate Browsing window.




Any browsing conducted within that window leaves no trace on the hard drive. For example, cookies and temporary Internet files are stored only in memory (they are cleared when you close the browser), and the URLs of the sites you visit are not recorded in the Web page history.

While many people may first think of InPrivate Browsing mode as a way to conceal visits to inappropriate Web sites on company time, the feature has legitimate business applications. For example, an HR employee may need to visit web sites that contain sensitive information such as financial or medical information; an IT employee may need to visit administrative Web sites that contain tools that control the organization's computer systems.

By using InPrivate Browsing, such Web sites can be accessed securely from any computer on the premises without leaving a trail after the browsing session is complete.

To open an InPrivate Browsing window, click the **Tools** button, point to **Safety**, then click **InPrivate Browsing**. You can also press CTRL+SHIFT+P to open an InPrivate Browsing window.

## Security Features

Because Web browsing can expose a system to malicious code, every Web browser includes built-in security features that help to keep the user safe while online. These built-in features control how the browser handles active content, scripts and Java programs.

Active content consists of any active, or moving, objects on a Web page, such as ActiveX controls and Java applets. Both ActiveX controls and Java applets allow information to be downloaded and run on your system, and there are inherent security risks with each. Internet Explorer can provide added security by controlling active content downloading and the execution of Java programs.

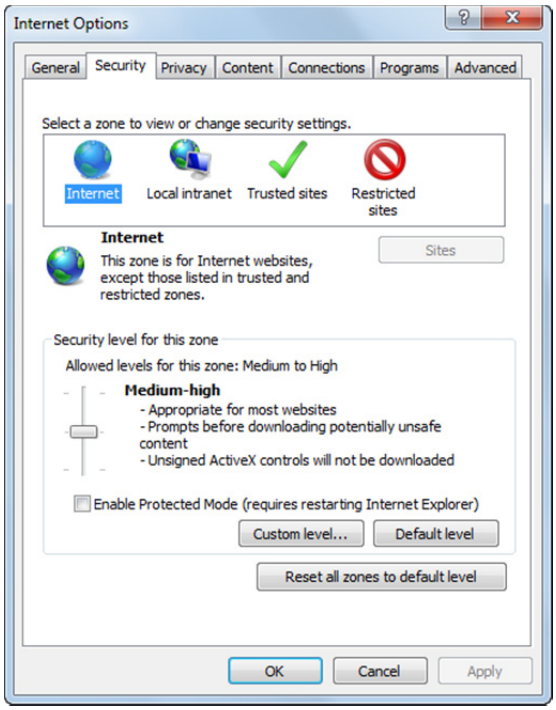
Some corporate IT departments require that company browsers be configured to disable all active content. Disabling these features reduces bandwidth use over the corporate network, and reduces security risks. However, certain Web page elements may not function as designed.

## Understanding Internet Security Zones

Internet Security zones offer a means of separating Web sites you trust from those that you do not trust. Each site has its own security settings. The four different security zones are as follows:

| | |
|---|---|
| **Internet** | Every Internet Web site you visit automatically falls into the Internet security zone unless you move it to another zone. The security level is set to Medium High by default, but you can change it to either Medium or High. |
| **Local intranet** | An Intranet is a private Web site maintained on a corporate network. It may be used for such activities as distributing documents, accessing company training or inputting information. Every Web site within the corporate intranet automatically falls into the Intranet Zone. The security level is set to Medium by default, but you can change it to any level. |
| **Trusted Sites** | Initially no sites fall into this category. You can add sites that you trust to this category so that you do not receive a security warning every time you visit the site. The security level is set to Medium by default, but you can change it to any level. |
| **Restricted Sites** | Initially, no sites fall into this category. You can move any Web site that you use but do not fully trust into this zone to enforce maximum security. The security level is set to High and cannot be changed. |

You can adjust the security settings of the various zones in the Security tab of the Internet Options dialog box. Click the **Tools** button, then click **Internet Options** to open the dialog box.



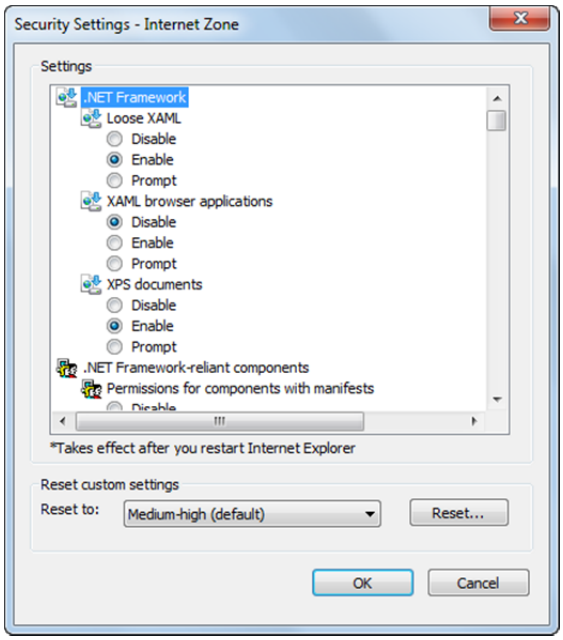

You can adjust the security level by dragging the slider bar.

Each safety level performs certain actions, depending on the content of the Web page. For example, if the security level is set to High, and a Web page with active content is encountered, the active content will not display and a notification message will appear. The High safety level does not give you the option to view the active content.

If the security level is set to Medium High, you may receive a warning message when you start to download a file. The message will give you the option to open the file in its current location, save it to your disk, cancel the download or request more information.

If the security level is set to Medium, you will still be prompted when downloading potentially unsafe content and unsigned ActiveX controls, but more content will be allowed through than with higher safety level settings.

You can also click the **Custom level** button to open the individual settings for the selected zone. You can use this dialog box to specify how to handle active content, downloads, scripts and authentication.




In situations where a site does not function properly with the Internet zone security settings applied, it is considered best practice to add that site to the *Trusted sites* zone, rather than lowering the settings for the Internet zone.

When you add a site to the Trusted sites zone, you will be limited to adding secure sites only to that zone. A secure site is one whose address starts with https:// rather than http://. You can, however, eliminate this restriction by clearing the Require server verification (https:) for all sites in this zone check box.

## SmartScreen Filter

The SmartScreen Filter is a feature in Internet Explorer that helps detect phishing Web sites and helps protect users from downloading or installing malware (malicious software).

Phishing is the process of trying to gather sensitive information such as a password, or credit card details from an unsuspecting victim by pretending to be a trustworthy entity. Typically, a phisher sends a legitimate-looking e-mail message that directs the recipient to visit a fake Web site that looks identical to a legitimate site. Victims are then asked to update personal information (such as password, credit card, or bank account numbers) on the fake Web site. The phisher can then use the captured information for malicious purposes.

SmartScreen Filter provides protection in the following ways:

- As you browse the Web, it analyzes Web Pages and searches for characteristics that might be suspicious. If it finds any suspicious characteristics, it will display a warning.
- It checks Web pages against a dynamic list of reported phishing sites and malicious software sites (maintained by Microsoft). If it finds a match, it will display a warning that says the site has been blocked for your safety. You can also report a Web site that you suspect might be unsafe.
- It checks files you download from the Web against a list of reported malicious software sites and programs known to be unsafe. It will warn you if it finds a match. It will also alert you if the file you are downloading is not on a list of well-known and often-downloaded files.

If a malicious site is detected, Internet Explorer 9 blocks the entire site. It can also exercise a "surgical block" of malware or phishing hosted on legitimate Web sites by blocking malicious pages without affecting the rest of the site.

SmartScreen Filter also works with Download Manager to help protect you from malicious downloads. Potentially risky downloads are blocked immediately. Download Manager clearly identifies higher risk programs so that the user can make an informed decision to delete, run, or save the download.

Sometimes sites are blocked inadvertently, and warnings may make users uncomfortable. If you know that a particular site is safe (for example, a site on a partner's extranet), but SmartScreen filter flags the site as suspicious, you can add the site to the list of Trusted sites within Internet Explorer, and then turn off checking for the Trusted sites zone.

Keep in mind that SmartScreen Filter interrupts the ability to navigate to and download from sites known to host malicious content. However, users can elect to ignore the warning and continue. (You can use Group Policy to prevent users from overriding the warning. You will learn about Group Policy in a later lesson.)

### Pop-Up Blocker

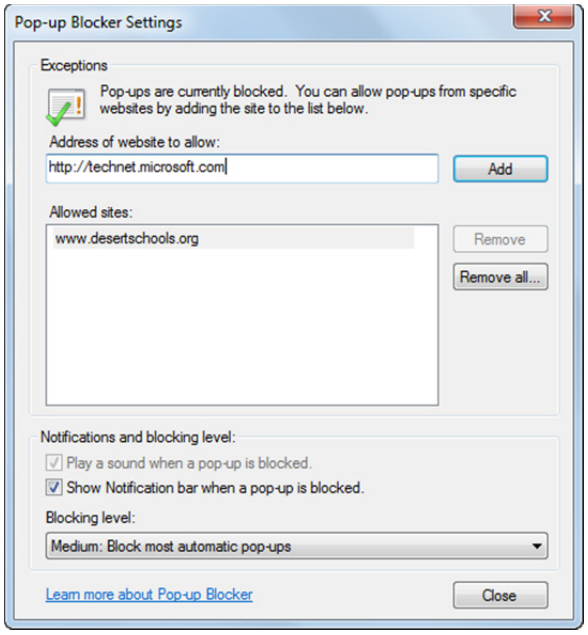
A pop-up is a small browser window that suddenly opens in front of the page you are viewing. Pop-ups contain command buttons or options that must be selected before you can continue with the current task. Pop-ups can remind a visitor to log on or to enter required information, but they are also used extensively for advertising on the Web, and many users find them annoying because they remain open until you click an option or manually close them.

Pop-up windows are also often used in connection with installing malware. Unsuspecting users may click links in a pop-up window that starts a download.

Internet Explorer provides a configurable pop-up blocker – you can fine-tune the way it functions so important messages (for example, log on windows, or session time-out warnings) are allowed to display. To allow pop-ups from particular Web sites, you add those sites to an exception list.

To access the pop-up blocker settings, click the **Tools** button, click **Internet options**, click the **Privacy** tab, select the **Turn on Pop-up Blocker** if necessary, then click the **Settings** button.

Type the address of the Web site you want to add to the exception list, then click the **Add** button.




Note that you can also specify the blocking level by selecting an option from the drop-down list.

**MMM**
Configuring Internet Explorer

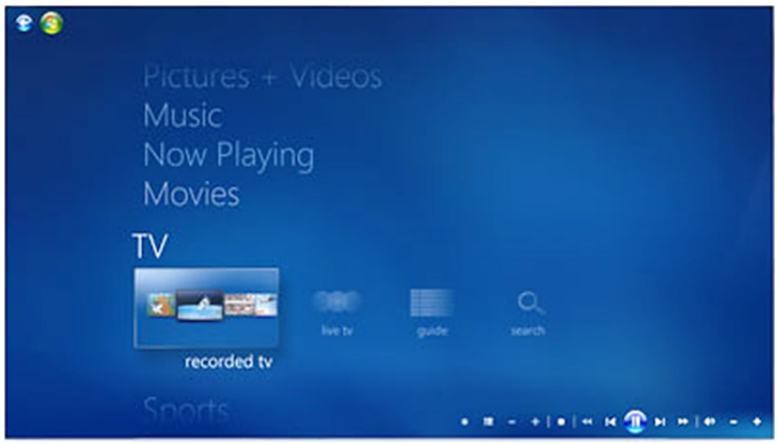
# Media in Windows 7

Objective 1.3

Video and audio are integral components of modern computing. Online tutorials, e-learning products, even customer service solutions include video and audio. Windows 7 provides two primary applications for handling media – Windows Media Player (WMP) and Windows Media Center (WMC)

## Windows Media Center (WMC)

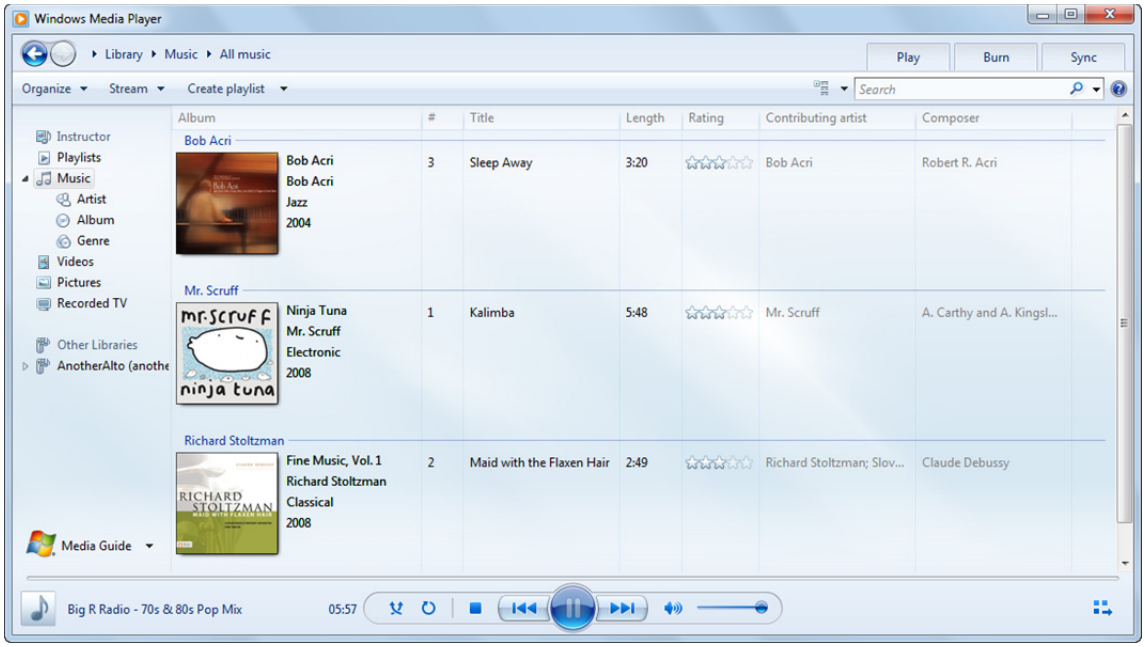
Windows Media Center is targeted at the home entertainment market. Windows Media Center can integrate with a TV tuner allowing users to watch, pause and record TV broadcasts. Users can also watch DVDs, listen to songs, watch online shows via Internet TV, and create and watch slide shows of their personal photos all from one central location. Media on one PC can be shared with other PCs running Windows 7 if the PCs are part of the same HomeGroup.




WMC is often used in full-screen mode and can be navigated using a remote control.

# Windows Media Player (WMP)

Windows Media Player is a media player and media library application. You can use it to play digital media files, organize your digital media collection, burn CDs, rip music from CDs, sync digital media files to a portable device (such as an MP3 player), and shop for digital media content from online providers. Windows Media Player 12 is the most recent version and is available only in Windows 7.




## Digital Media and Digital Rights Management (DRM)

Digital Rights Management (DRM) is a technology used by content providers to control how digital music and video files you obtain from them are used and distributed. Some online stores sell and rent songs and movies that have DRM applied to them. A file that has DRM applied to it is considered a protected file. In Windows Media Player, DRM is known as Windows Media Digital Rights Management.

Media usage rights are permissions to use a protected file in specified ways. For example, usage rights might allow you to play a file (a play right), burn the file to an audio CD (a burn right), or to sync the file to a portable device (a sync right). These rights are sometimes called licenses.

When you purchase and play songs or videos, WMP automatically downloads the usage rights (DRM) as required.

When you try to use a protected file in Windows Media Player, the Player checks to see if you have valid media usage rights installed on your computer. If the media usage rights permit you to perform the action you have requested, the Player performs that action for you. If the Player does not find valid media usage rights, or if the rights do not permit you to perform the requested action, the Player will not perform the action, and typically displays an error message or an information button that you can click for more information.

## Supported Formats

The default file formats are Windows Media Video (WMV), Windows Media Audio (WMA), and Advanced Systems Format (ASF), but WMP supports most popular audio and video formats (e.g., MP3, MPEG-4, AVI, MOV).

WMP also supports playlists in a format called Windows Playlist (WPL).

## Business Uses

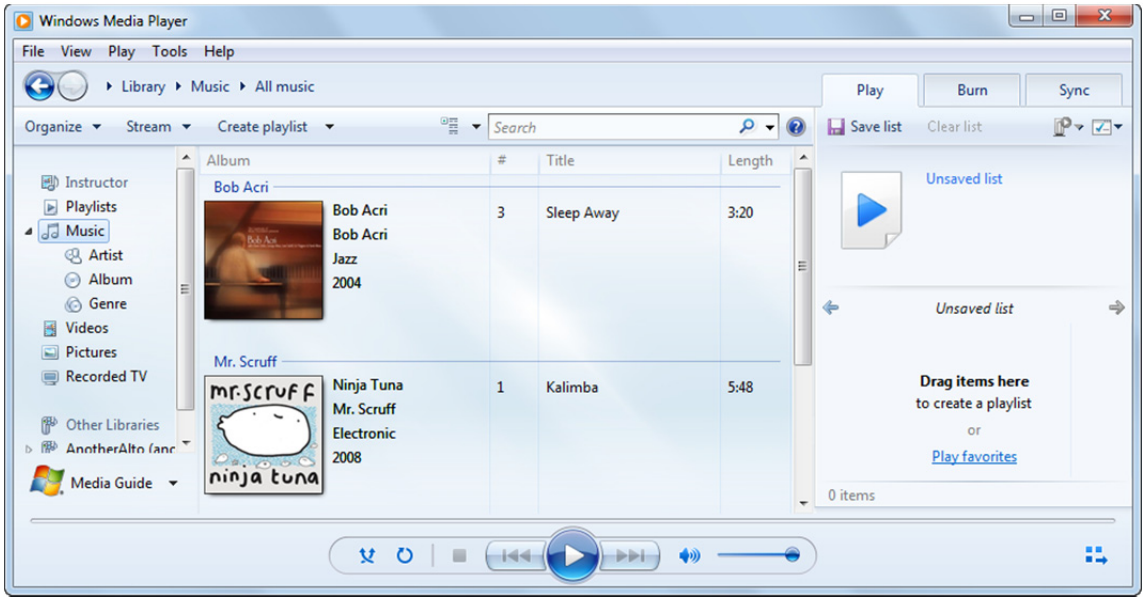
While WMC is intended for home entertainment, WMP has several practical business applications. Many Web sites use the WMP engine to embed media into their Web pages, and WMP is used to play streaming media.

WMP is used in businesses every day for e-learning applications, online tutorials, and other Web-based training.

## Player Library and Now Playing mode

In WMP, you can toggle between two modes: the Player Library (which provides control over the Player's features) and Now Playing mode (which provides a simplified view of the media and is ideal for playback).

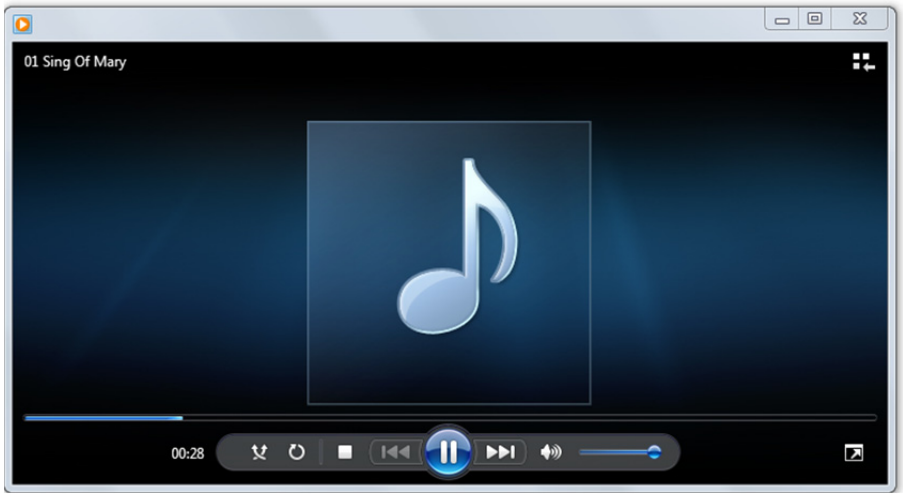
In Player Library mode (shown below) you can configure player options and organize your media files. When you open WMP from the Start menu, it opens in Player Library mode.




Within the Navigation pane (left pane), you can choose a category (such as Music, Pictures, or Videos) to view in the details pane (center pane). You can also drag items from the details pane to the list pane (right pane) to create playlists, burn CDs or DVDs or sync to devices such as portable music players.

You can play media in either mode. You can also start playing media in one mode and switch to the other mode. To switch from Player Library mode to Now Playing mode, click the Switch to Now Playing button in the lower-right corner of the WMP window.

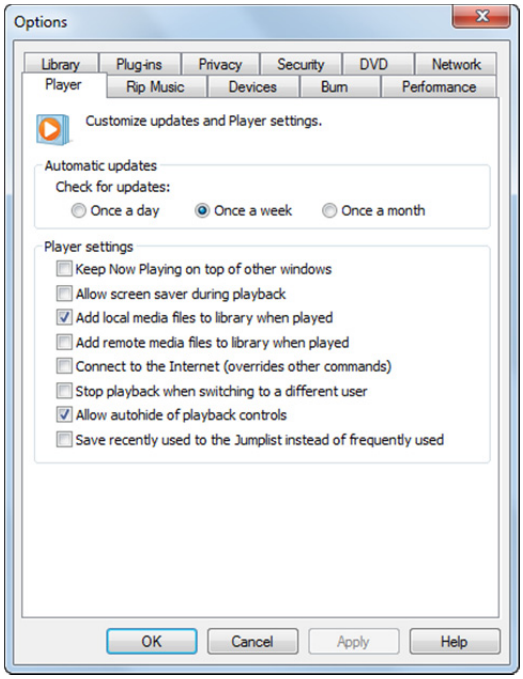
Now Playing mode is the mode most often used for playback. When you double-click a media file, or begin streaming media from a Web site, WMP opens in Now Playing mode (shown below).




To switch from Now Playing mode to Player Library mode, click the Switch to Library button at the upper-right corner of the WMP window.

## Configuring WMP

You can use the Options dialog box to configure WMP. To access the Options dialog box, press CTRL+M if necessary to make the menu bar visible, then select **Tools**, **Options**.




The Windows Media Player Options dialog box contains the following tabs:

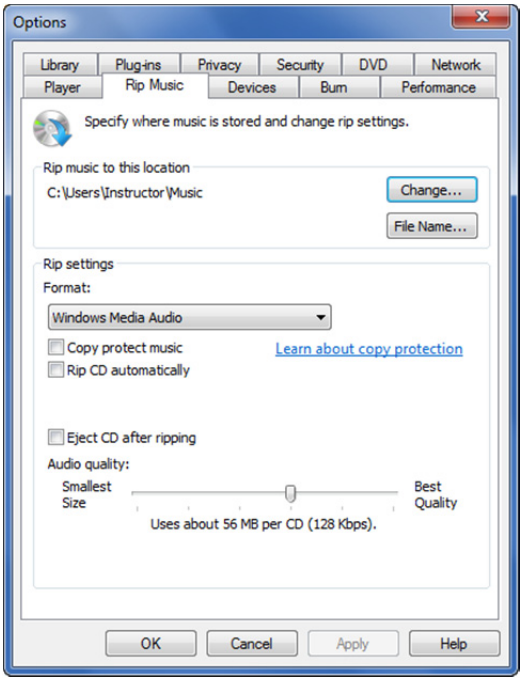
| | |
|---|---|
| **Player** | Contains settings for the player, including when to check for updates. |
| **Rip Music** | Ripping is the process of adding music to the Player Library by copying audio files from a CD and storing them as digital files on the computer. This tab includes settings for file formats and file locations. |
| **Devices** | Contains settings for optical drives, the display and speakers. |

| | |
|---|---|
| **Burn** | Contains settings for burning audio and data discs, including burn speed and whether to eject the disc after burning. |
| **Performance** | Contains settings for detecting the connection speed for streaming media, network buffering and DVD and video playback. |
| **Library** | Contains settings for organizing the digital media collection on the computer, including whether to retrieve additional information pertaining to media content from the Internet. |
| **Plug-ins** | Allows you to add and configure WMP plug-ins. |
| **Privacy** | Contains settings for automatically retrieving media information from the Internet, downloading usage rights, and sending Player usage data to Microsoft. |
| **Security** | Contains settings for running scripts and accessing security zone settings. |
| **DVD** | Contains settings that affect DVD playback, such as playback restrictions based on content rating, and language selection for audio, subtitles and DVD menus. |
| **Network** | Contains settings for playing streaming media, such as which network protocols to use and whether media is streamed through a proxy server. |

## Exercise 2-7: Exploring Windows Media Player Settings

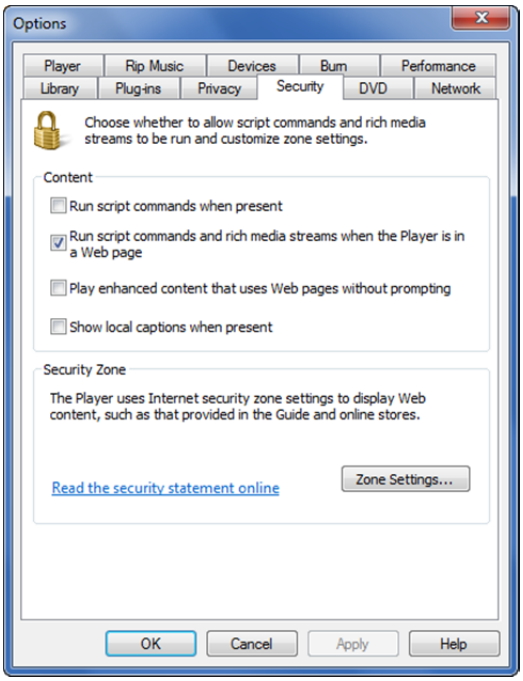

In this exercise, you will examine some of the configuration settings for Windows Media Player.

1. Click the **Start** button, click **All Programs**, then click **Windows Media Player** to open the Player.
2. If necessary, press CTRL+M to show the Menu bar.
3. Double-click one of the music files to begin playback. Notice that the file is added to the Playlist area of the Player.
4. In the Menu bar, click **Tools**, then click **Options** to open the Options dialog box.
5. In the Player tab, select **Once a month** as the Check for updates setting. How can this setting affect network bandwidth usage?
6. In the Player settings area, select the **Stop playback when switching to a different user** option, and deselect **Allow autohide of playback controls**. How do you think these settings will affect users?
7. Click the **Rip Music** tab.

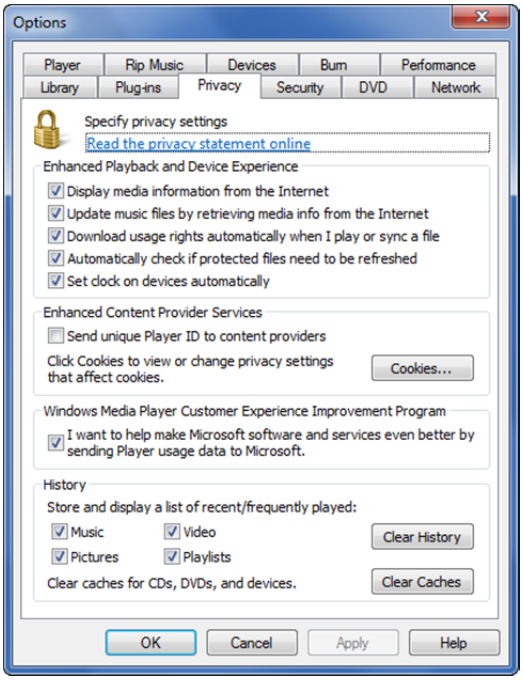



8. In the Rip settings section, display the **Format** drop-down list to view the available file formats, then click in an empty area of the dialog box.

9. In the Audio quality section, drag the slider to the left and to the right so see how increasing or decreasing the sound quality affects the storage requirements.
10. Click the **Library** tab. Notice that the default setting is to add video files found in the Picture library.
11. Click the **Security** tab. Notice that by defaults scripts are run only when the Player is in a Web page.




12. Click the **Privacy** tab and examine the settings. Do you think most users are comfortable sending Player usage data to Microsoft?




13. Click **Cancel** to abandon the revised settings, then close Windows Media Player.

In this exercise, you examined some of Windows Media Player's configuration settings.

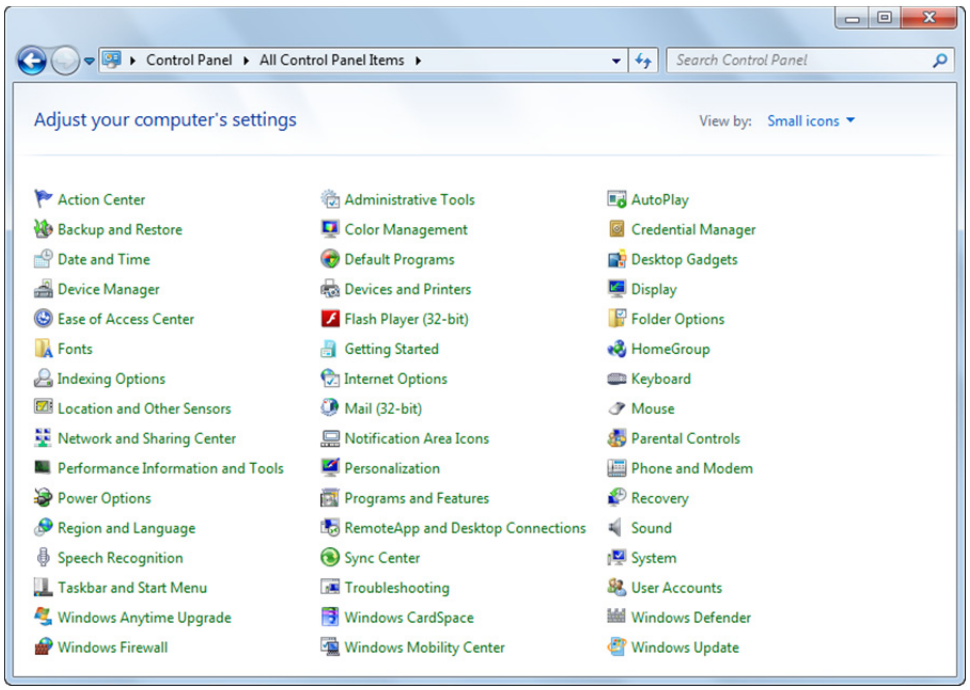
# Configuring Control Panel Options

Objective 1.1

The Control Panel consists of executable programs, components called applets (special Windows applications used to configure some aspect of the system), and Web pages that contain links to the various executable programs. The Control Panel brings order to these programs and configuration tools.

The Control Panel can be displayed in either Category view or Icons view. Category view is useful if you know what you want to do, but don't know the name of the specific applet or program you need to access. Category view is shown below. You can click the links presented in Category view until you drill down to the exact applet or program you need.

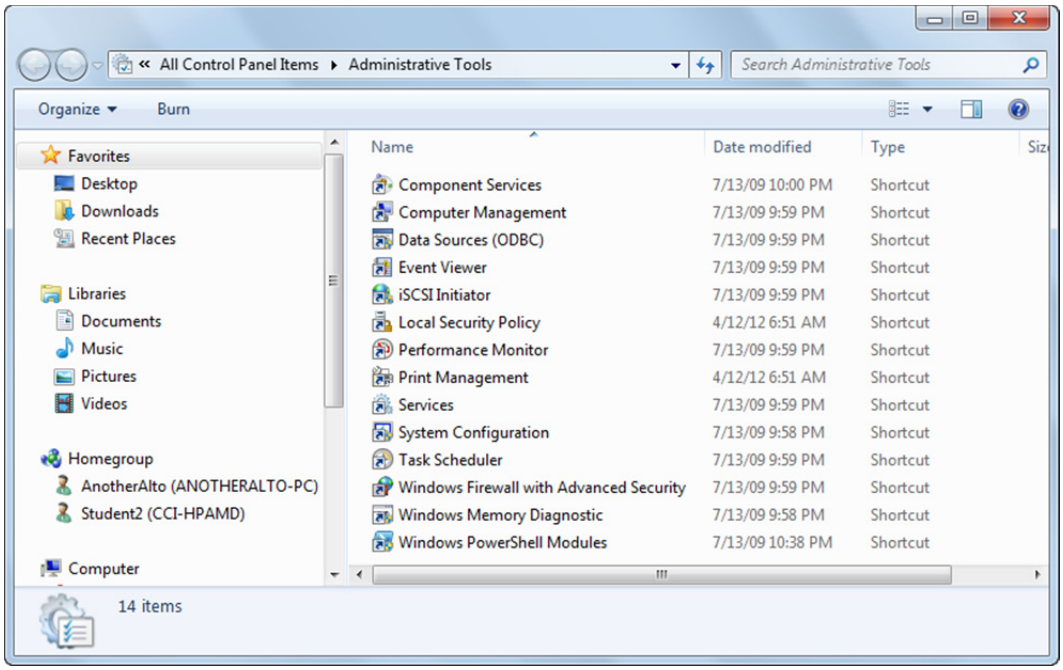

Icons view presents an alphabetical listing of the Control Panel components. You can specify to show large icons or small icons. Icons view is shown below.




You can browse the Control Panel or use the Search box at the top of the window to find the tool you need.

# Configuring Administrative Tools

All Windows operating systems include a special set of tools that have been traditionally called Administrative tools. These tools allow you to manage the system configuration and typically require administrative privileges to operate. The Administrative tools are shown below.




The administrative tools are:

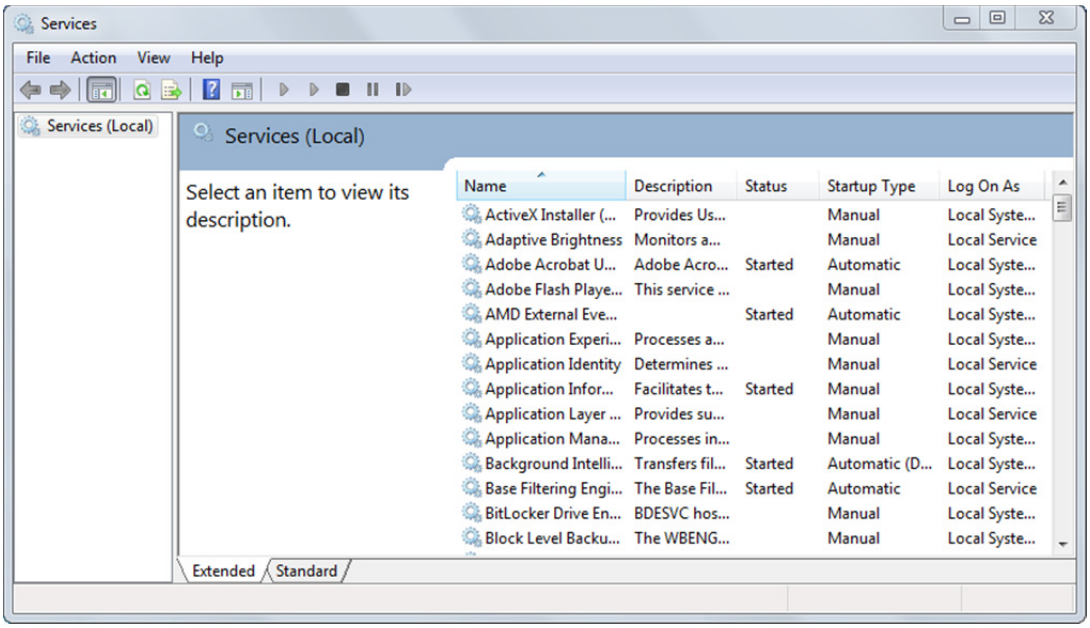
| | |
|---|---|
| **Component Services** | Configure and administer Component Object Model (COM) components. Microsoft COM technology enables software components to communicate. COM is used by developers to create re-usable software components, link components together to build applications, and take advantage of Windows services. |
| **Computer Management** | Provides a single, consolidated desktop tool that you can use to monitor system events, manage system performance, and view and control devices. |
| **Data Sources (ODBC)** | Used to move data from one type of database into another. |
| **Event Viewer** | Allows you to view event logs. Logs provide a record of specific events that take place in a computer system. |
| **iSCSI Initiator** | Used to configure and manage the Internet Small Computer Systems Interface (iSCSI) Initiator – a device driver and service in Windows 7 that allows access to iSCSI-based storage area networks (SANs). |
| **Local Security Policy** | Allows you to easily access the security settings for the local computer. |
| **Performance Monitor** | Allows you to view information about the CPU, memory, hard disk and network performance. |
| **Print Management** | Allows you to manage printers and print servers on the network. You can also view drivers and manage print queues. |
| **Services** | Allows you to view the services that run in the background on the computer. (A service is a program or process that runs in the background and provides support to other programs.) |
| **System Configuration** | Opens the System Configuration tool which is a utility in Windows 7 that you can use to identify and isolate problems that may prevent Windows from starting correctly. |
| **Task Scheduler** | Allows you to schedule programs or other tasks to run automatically. |
| **Windows Firewall with Advanced Security** | Allows you to configure firewall settings on the local machine and on remote systems. (A firewall is hardware or software that protects a computer from hackers and malicious software.) |

| | |
|---|---|
| **Windows Memory Diagnostic** | Runs a diagnostic program that will check the system memory to ensure that it is functioning correctly. |
| **Windows PowerShell Modules** | Runs a PowerShell session with all available modules loaded automatically. (You will learn about PowerShell in a later lesson.) |

## Exercise 2-8: Using Administrative Tools

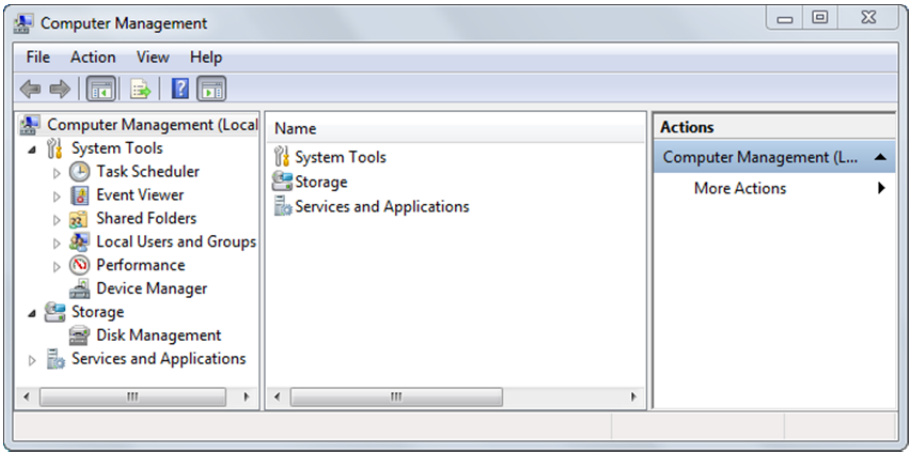
In this exercise, you will navigate the Control Panel and explore some of the administrative tools.

1. Click the **Start** button, then click **Control Panel** to open the Control Panel home page. If necessary, display the View by drop-down list, then select **Category** to apply Category view.
2. Click a few of the category links to see if you can find the administrative tools. If you open the Administrative Tools window, close it. (You will investigate the tools shortly, but should practice navigating the Control Panel first.)
3. In the left pane, click the **Control Panel Home** link.
4. Click in the Search box at the top of the window, then type: `admin` to view the pertinent links.
5. At the top of the window, click the **Back** button to return to the Control Panel home page.
6. Display the View by drop-down list, then select one of the icon views.
7. Click the **Administrative Tools** link.
8. Close the Administrative Tools window.
9. Display the View by drop-down list, then select **Category** view.
10. Click the **System and Security** link, then click the **Administrative Tools** link to view the administrative tools again.
11. In the right pane, double-click **Windows Firewall with Advanced Security** to view the current firewall settings.
12. Close the Windows Firewall with Advanced Security window to return to the Administrative Tools window.
13. In the right pane, double-click **Services** to view the services that run in the background on the computer.




14. Scroll the list of services. Are you surprised at how many there are? If the status of a service is *Started*, then the service is running. Any service with a startup type of Automatic should be running on the system.

15. Click the name of a service to display its description in the dialog box. Some services include Start, Stop and Restart links, allowing you to control how they run. (You will learn more about services in a later lesson.)
16. Close the Services window.
17. In the right pane, double-click **Event Viewer** to view information about significant events, such as a program starting or stopping, or a security error.
18. Maximize the Event Viewer window and explore a few of the logged events. Are there more errors and warnings than you had expected?
19. Close the Event Viewer window.
20. In the right pane, double-click **Computer Management** to open the Computer Management console. Notice that you can perform a wide variety of tasks from this one location.




21. Close the Computer Management console.
22. Close the Administrative Tools, then close the Control Panel.

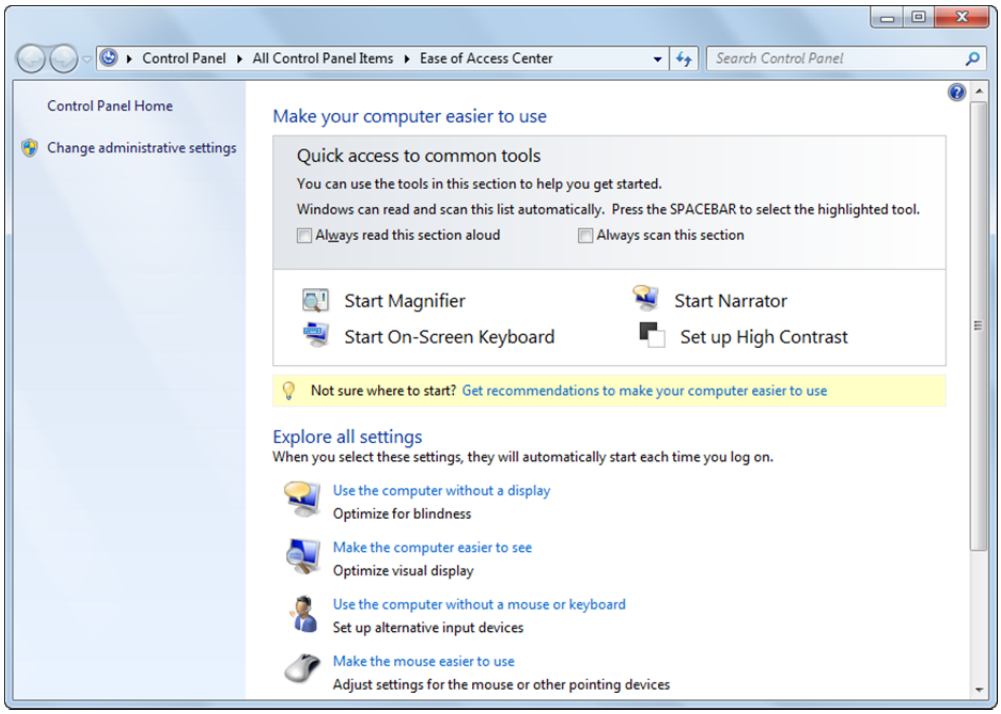
In this exercise, you navigated the Control Panel and explored a few of the administrative tools.

You can find more information on administrative tools on the TechNet Web site at:
http://technet.microsoft.com/en-us/default.aspx?ocid=fwlink

## Configuring Accessibility Options

Accessibility is key in modern-day computing; there has been significant legislation to ensure that people with disabilities (e.g., vision impairment, hearing loss or physical challenges) can have useful experiences with computers. Windows 7 includes accessibility options and programs that make it easier to see, hear and use the computer.

The Ease of Access Center provides a centralized place to locate accessibility settings and programs. You can access it through the Control Panel, or by pressing WINDOWS LOGO key+U.




The Ease of Access Center includes:

- Quick access to accessibility tools such as Magnifier, On-Screen Keyboard, Narrator and High Contrast.
- A questionnaire that provides a personalized list of recommended settings based on the answers to a series of questions regarding the user's eyesight, dexterity and hearing.
- Settings that are organized by category. For example, you can find how to use the computer without a display, or how to make the mouse easier to use, or how to use text or visual alternatives to sound.

## Common Accessibility Tools

Common accessibility tools in Windows 7 are described in the following table:

| | |
|---|---|
| **Magnifier** | Enlarges portions of the screen making it easier to view text and images and see the whole screen more easily. In Windows 7, Magnifier includes full-screen mode, lens mode and docked mode. You can set the magnification level up to 16 times the original size. |
| **On-Screen Keyboard** | Displays a visual keyboard on the screen. Instead of using the physical keyboard to type and enter data, you can use the On-Screen keyboard to select keys using the mouse or another pointing device. The keyboard can be resized and customized to make it easier to see and use. It also includes text prediction, which displays a list of words that you might be typing as you enter the first couple of letters. Text prediction is available in eight languages. |
| **Narrator** | Narrator is a basic screen reader which reads aloud text on the screen and describes some events (such as the appearance of error messages) to let you know what is happening as you use the computer. |
| **Set up High Contrast** | Increases the contrast in colors to reduce eyestrain and make things easier to read. You can turn on this feature by pressing LEFT SHIFT+LEFT ALT+PRINT SCREEN. The High Contrast Windows themes can be used for this feature. |

## Other Accessibility Tools and Features

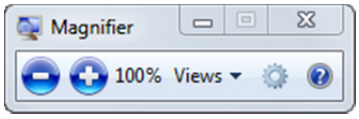
Windows 7 includes several other accessibility tools and features. You have already investigated some of these when you configured display settings. Others include:

| | |
|---|---|
| **Speech Recognition** | Allows you to command your PC with your voice, including the ability to dictate into almost any application, such as Microsoft Word or Microsoft Excel, or Microsoft Outlook. You can also surf the Web by saying what you want to see. Speech recognition requires a microphone. The setup process is streamlined and an interactive tutorial is available to help you familiarize yourself with speech commands. |
| **Windows Touch** | Allows you to use a touchscreen monitor to scroll, resize windows, play media, pan and zoom. |
| **Sticky Keys** | When turned on, this feature allows you to press one key at a time to enter key combinations (such as CTRL+ALT+DELETE). |
| **Mouse Keys** | Allows you to use the arrow keys on the numeric keypad to move the pointer instead of the mouse. |
| **Filter Keys** | Ignores keystrokes that occur in rapid succession and keystrokes that are held down for several seconds unintentionally. |
| **Visual Notifications** | Replaces system sounds with visual cues, such as a flash on the screen, so that system alerts are announced visually instead of aurally. |

## Exercise 2-9: Configuring Accessibility Options

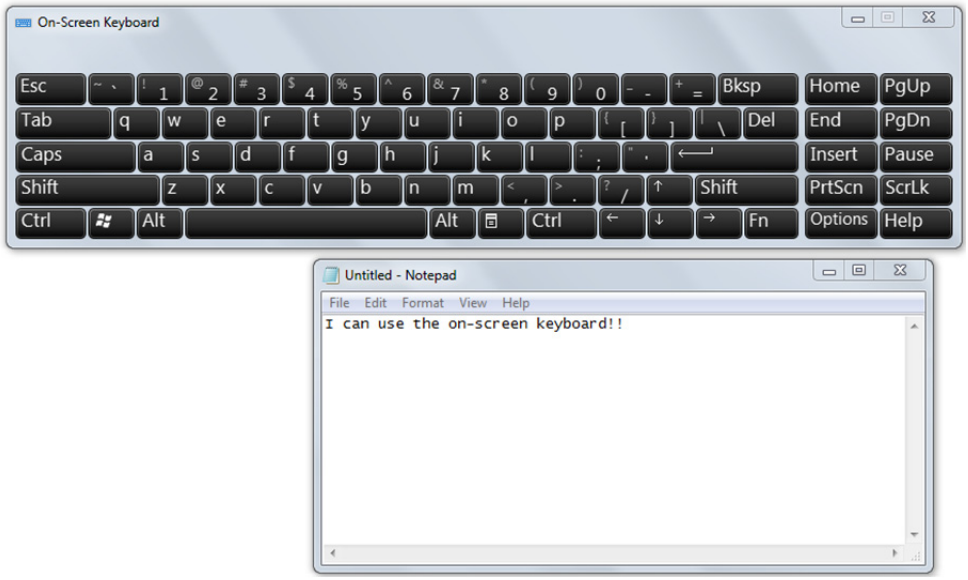

In this exercise, you will work with options in the Ease of Access Center.

1. Click the **Start** button, then click **Control Panel** to open the Control Panel window.
2. If necessary, set the View by option to **Large icons**, then click **Ease of Access Center**.
3. In the Ease of Access Center, click **Start Magnifier**. Windows starts Magnifier and displays the Magnifier toolbar. Use the options on the toolbar to set the mode and magnification level.

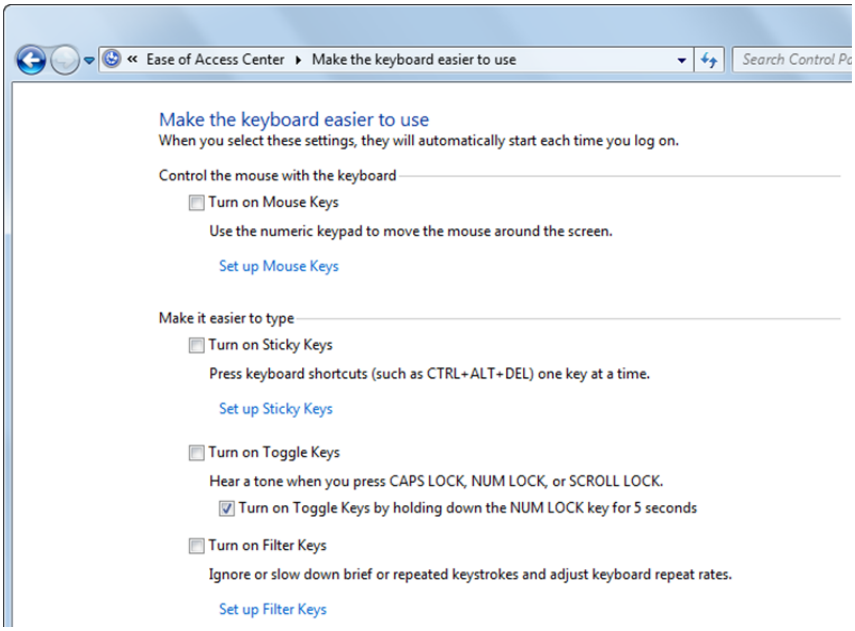



**MMM**
Configuring Voice Recognition

4. In the Magnifier toolbar, display the Views drop-down list, then select **Lens**. (Note that Lens is not available if you are not using an Aero theme.) Magnifier displays a rectangular frame which will act as a magnifying glass as you move it around the screen.
5. In the Magnifier toolbar, click the **Zoom in** button twice to increase the magnification level to 300%. If the Magnifier toolbar is not visible, click the magnifying glass icon to make the toolbar appear.
6. Move the magnifying lens around the screen.
7. In the Magnifier toolbar, click the **Zoom out** button once to reduce the magnification to 200%.
8. Change the view to Full screen and move the mouse around the Desktop.
9. In the Magnifier toolbar, click the **Close** button to turn off the Magnifier.
10. In the Ease of Access Center, click **Start On-Screen Keyboard**. Windows opens the On-Screen Keyboard.
11. In the On-Screen Keyboard, click the WINDOWS LOGO key once or twice as necessary to open the Start menu, then use the mouse to open the Notepad application.
12. Use the On-Screen Keyboard to enter text into the new Notepad document.




13. Close the Notepad document without saving, then drag a corner or an edge of the On-Screen Keyboard. Notice you can make it as large or small as you want.
14. In the On-Screen Keyboard, click the **Close** button.
15. In the Ease of Access Center, scroll down and click the **Make the keyboard easier to use** link to display the available options. Notice that you can set up mouse keys, set up sticky keys, turn on toggle keys and set up filter keys.




16. Click the **Back** button at the top of the window to return to the Ease of Access Center.
17. Investigate some of the other links in the Ease of Access Center.
18. In the Ease of Access Center, click the **Get recommendations to make your computer easier to use** link to take the interactive questionnaire. Indicate that you have some type of impairment so that Windows can make specific recommendations based on your answers. When you are done, review the recommended settings. Did you know that the suggested configurations were possible?
19. Close the Ease of Access Center.

In this exercise, you investigated settings in the Ease of Access Center.

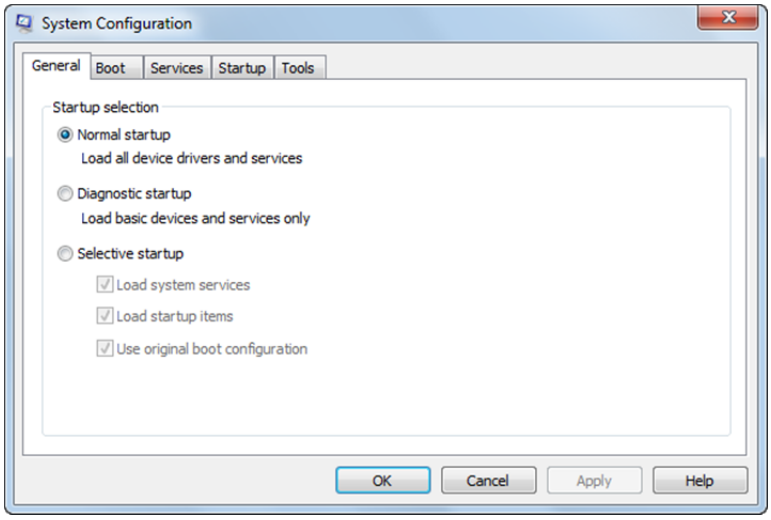
# Using the System Configuration Tool

Objective 1.3

The System Configuration tool (called MSCONFIG) is a utility in Windows 7 that you can use to identify and isolate problems that may prevent Windows from starting correctly.

You can use MSCONFIG to start Windows with common services and startup programs turned off and then turn them back on, one at a time. If a problem doesn't occur when a service is turned off, but does occur when that service is turned on, then the service could be the cause of the problem.

The System Configuration dialog box is shown below.




The System Configuration dialog box includes the following tabs:

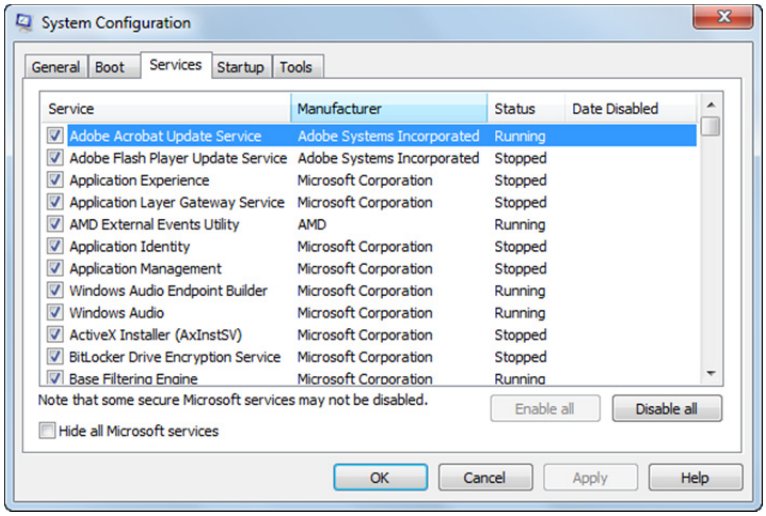
| | |
|---|---|
| **General** | Lists choices for startup configuration, including Normal, Diagnostic and Selective startup. |
| **Boot** | Shows configuration options for the operating system. For example, you can boot into safe mode and load only particular drivers, and specify to work in a GUI or a command-line environment. You can also specify whether networking is enabled. |
| **Services** | Lists all of the services that start when the computer starts, along with their current status (Running or Stopped). You can enable or disable individual services at startup to troubleshoot which services might be causing startup problems. |
| **Startup** | Lists applications that run when the computer starts up, along with the name of their publisher, the path to the executable file, and the location of the registry key or shortcut that causes the application to run. (You will learn about registry keys in a later lesson.) |
| **Tools** | Presents a list of diagnostic and other advanced tools. You can launch the tools from the dialog box. |

## Exercise 2-10: Using MSCONFIG

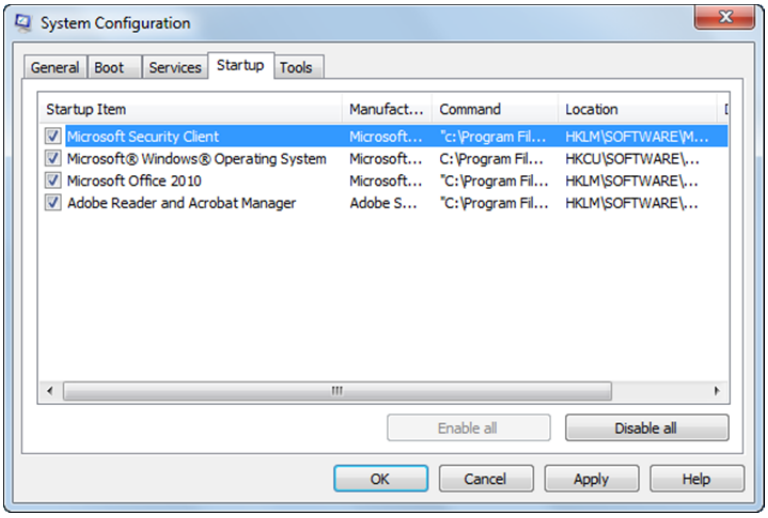

In this exercise, you will explore some of the tools in the System Configuration tool (MSCONFIG).

1. Click the **Start** button, click in the Search box, type: `msconfig.exe` then press ENTER.
2. If necessary, enter the administrator password to allow the program to launch.

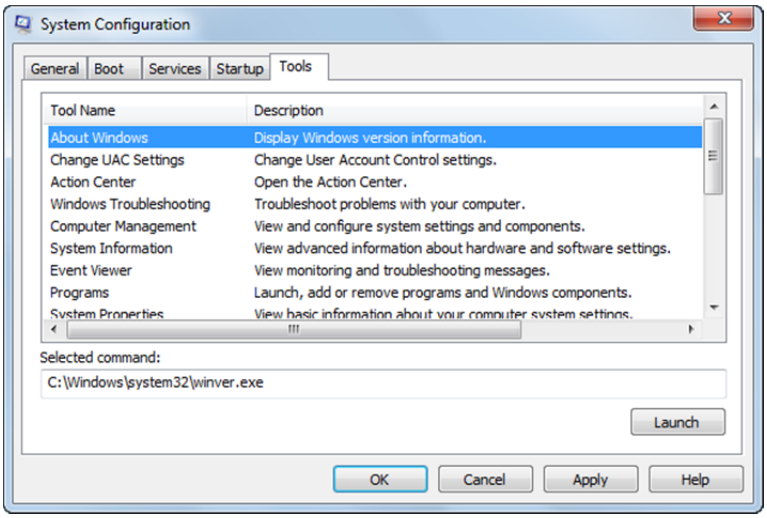
3. Click the **Services** tab to view the services that start when the computer boots up. By default, all are enabled.




4. Click the **Disable all** button to clear all the checkboxes. You can add services back in one by one, or you can enable them all and then remove services one by one.
5. Click the **Enable all** button to reselect the checkboxes.
6. Select the **Hide all Microsoft services** option. Now the list displays only third party services that are started at bootup.
7. Clear the **Hide all Microsoft services** checkbox, then click the **Startup** tab to view the applications that run when the computer starts up. You can clear the check boxes to prevent these programs from starting in order to see if one of them might be causing trouble at bootup.




8. Click the **Tools** tab to view the available tools. You can launch tools directly from the System Configuration dialog box.




9. In the list box, click **System Properties**, then click **Launch** to open the System page of the Control Panel. This screen shows information about the system, including the operating system edition, the processor speed, the bit-level, etc. Close the Control Panel window.
10. In the list box, click **Internet Options**, then click **Launch** to open the Internet Properties dialog box used to configure Internet Explorer. Close the Internet Properties dialog box.
11. In the list box, click **Command Prompt**, then click **Launch** to open a command prompt window. Close the command prompt window.
12. Explore a few of the available tools. (However, avoid launching the Registry Editor. You will use the Registry Editor under controlled conditions in a later lesson.)
13. When you are done, close the System Configuration dialog box.

In this exercise, you explored some of the tools in the System Configuration tool (MSCONFIG).

# Understanding Mobility

Objective 1.4 4.4

Mobile computing occurs when a computer is transported from location to location as part of its normal usage. Mobile users are everywhere; you see them in airports and train depots and local coffee houses with their laptops at the ready.

Mobility has become increasingly important for business users – and not only for those who travel extensively as part of their job. More and more, users are taking their portable PCs home so they can work after hours or over the weekend.

Most business users work with files that are stored in a shared folder on their company's network. If mobile users require access to those files while they are away from the network, they can use offline files. Offline files are copies of network files stored on the local machine (or on removable media) so that they can be accessed even when mobile users are away from the network.

Once users save their changes to these offline files, the operating system must provide a method for synchronizing this revised offline content with the network. In Windows 7, you can use the Windows Sync Center.

Another aspect of mobility is that laptops are used more than ever today. You can use the Windows Mobility Center to help prolong battery life and make connectivity with other devices fast and easy.

## Windows Sync Center

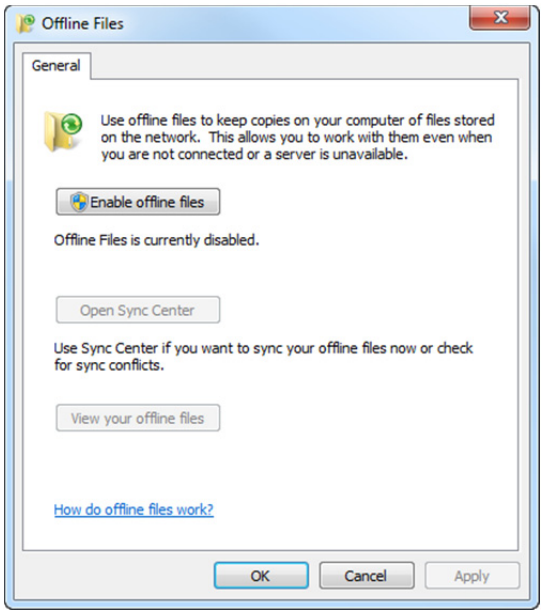
If you require access to network files while your computer is not connected to the network, you can use offline files. When you make network files available offline, a copy of the network files are created on your computer and these copies are called offline files. Offline files are available to mobile users at all times.

After you make changes to your offline files, Windows will automatically synchronize the offline files with the original files in the network folder the next time you connect to the network.

**Note:** Sync Center is designed to help you sync with files in network locations. If you want to sync a mobile device with your computer, such as a mobile phone or portable music player, Windows provides other options. You can install the sync software that some manufacturers include with their devices, or you can use the new Device Stage feature in this version of Windows if your device supports this feature.

## Setting Up Offline Files

By default, this feature is turned off in Windows 7. To enable it, go to the Control Panel, click on Sync Center, and click Manage offline files in the left pane of the Control Panel. Click on Enable offline files, and reboot your computer.

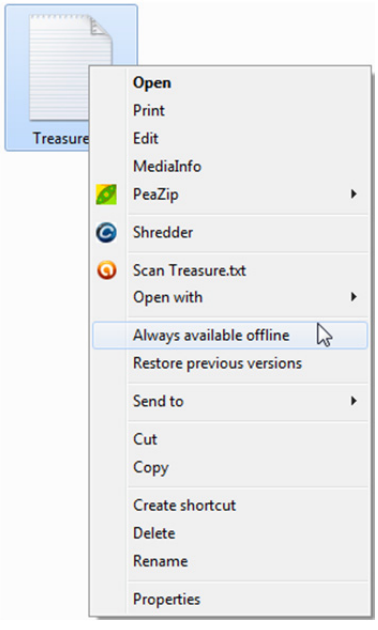



This feature is only available in the Professional, Enterprise, and Ultimate editions of Windows 7, and Windows Server 2003 and later versions.

## Making Files Available Offline

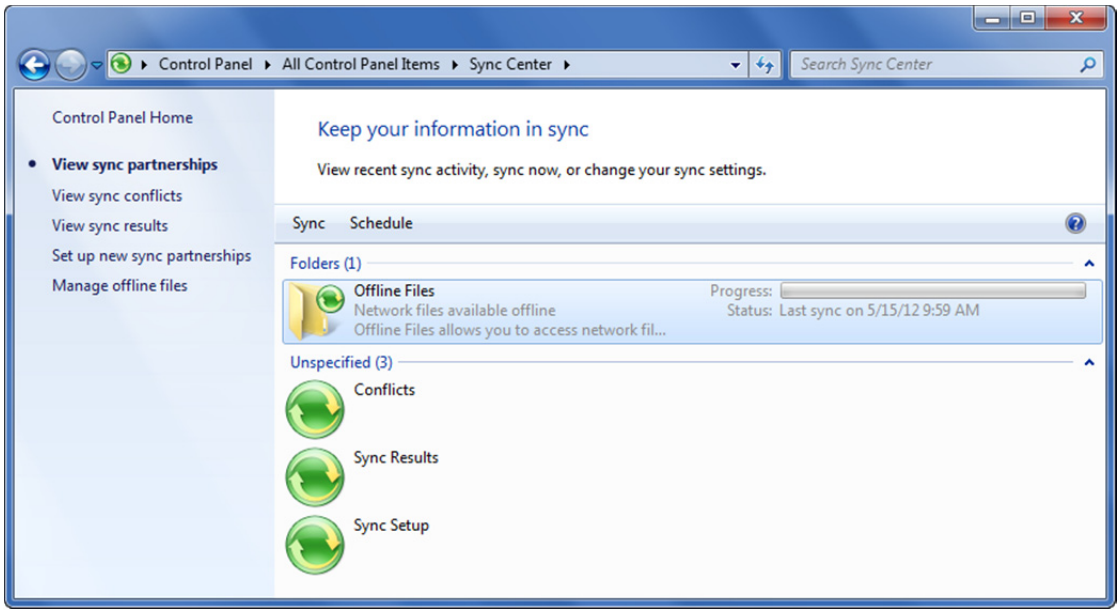
To make a network file available offline, simply select the file on the network, right-click, then select **Always available offline**.

Windows automatically creates a copy of the file on your computer. The next time you try to access this file, you will be able to open it even if the network version is unavailable. You can now work with the offline file just as you would any other file.



## Synchronizing Files with the Network

The next time you connect to the network, Windows will automatically sync your offline files with the original files in the network folder.




You can also manually synchronize the files, or schedule a synchronization to occur at a specific time or when an event (such as logging on to the computer) occurs.

If conflicts occur when you synchronize files, the Sync Center can help you to resolve them. A synchronization conflict may happen when you have more than one person sharing the same folder and working on the same file and all want to synchronize.

When you perform synchronization, any conflicts are clearly indicated so that you can choose whether to view options to resolve the conflict, ignore it or view the properties of the conflict.

## Exercise 2-11: Using Offline Files (Optional)

In this exercise, you will make changes to a file that is located on a remote computer that is offline, and then synchronize it when the remote computer becomes available again. Note that this exercise assumes your computer is already configured to make files available offline, and that you are able to access a remote computer that you can shut down and start up again. For the purpose of this exercise, the remote computer will be referred to as a server, but it can also be any desktop or laptop computer running Windows 7 Professional or higher, or Windows Server 2003 or later versions.

For this exercise, pair up with a lab partner. One person will perform the "server" steps and the other will perform the "computer" steps, even though both parties will be using Windows 7 client systems.

First, you will create and share a directory on the server.

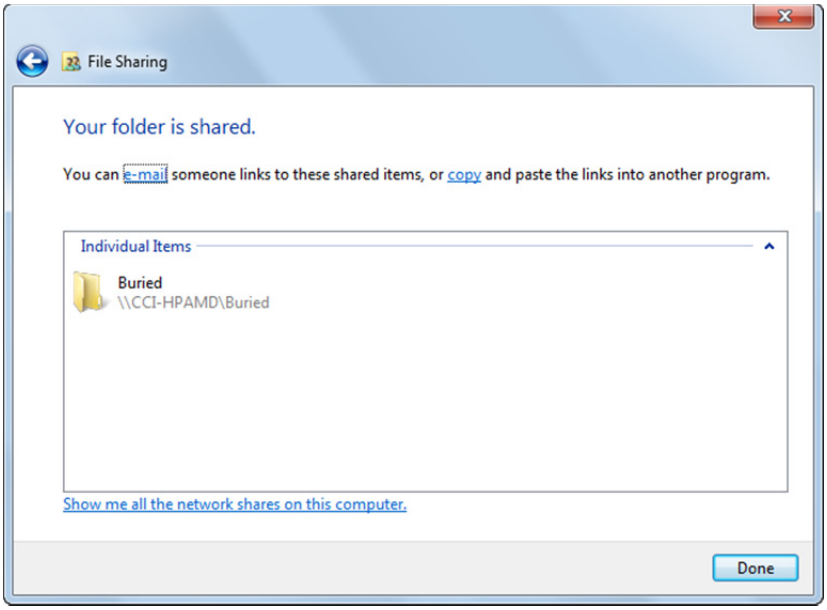
1. **Server**: Open Windows Explorer and create the directory Buried on the root directory of drive C. The path for the directory should be C:\Buried.

The security settings of this directory must be reconfigured so that you can add and update files from another computer.

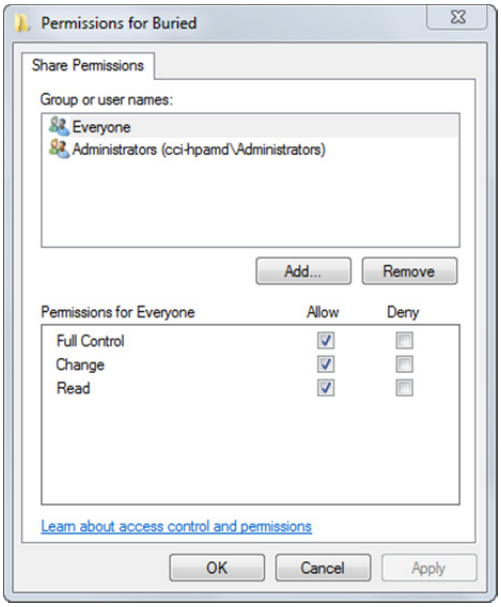
2. Right-click the Buried directory and click **Properties**.
3. Click the **Sharing** tab, then click the **Share** button to launch the File Sharing wizard.
4. Display the drop-down list, select **Everyone**, then click the **Add** button to add the Everyone local security group to the list of people you want to share with.

   Note that you may not want to use the Everyone security group in a corporate network – it allows everyone to access the directory and its contents. It is used in this exercise for simplicity purposes only.

5. Display the Permission Level drop-down list for the Everyone group, then select **Read/Write** to change the permission from Read to Read/Write.
6. Click the **Share** button. When the File Sharing wizard has completed configuring the folder, it will display a message that the folder is shared.

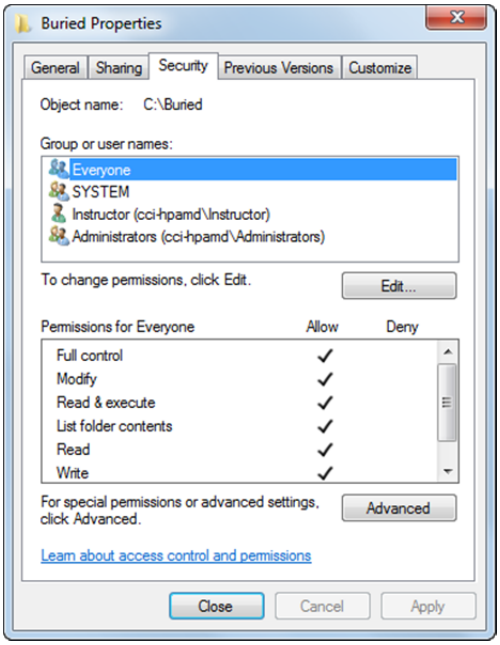



7. Click **Done** to close the File Sharing wizard and return to the Sharing tab of the Properties dialog box.
8. Click the **Advanced Sharing** button to open the Advanced Sharing dialog box, then click the **Permissions** button to view the share permissions for the directory. Notice that the Everyone group has Full Control permissions.




9. Click **OK** twice, then click the **Security** tab.

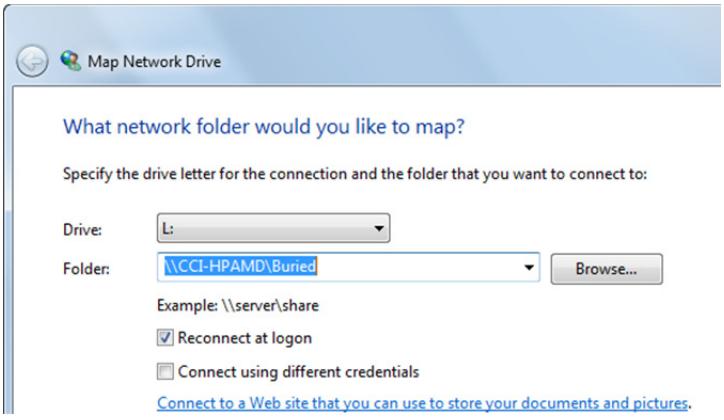
10. In the Group or user names list box, click **Everyone**, then examine the applied permissions in the Permissions for Everyone box at the bottom of the tab. If there is no check mark in the Allow column for the Full Control permission, click the **Edit** button, click the **Allow** check box for the Full Control permission, then click **OK**. The Buried directory is now a network share. The Security tab should appear as shown below:




11. Close the Properties dialog box.

Now map the Buried directory to your computer so that you can access it from there.

12. **Computer**: Open Windows Explorer.
13. If necessary, click **Computer** in the left pane, then click **Map network drive** in the menu bar.
14. Click the **Drive** drop-down button and select a drive letter that is available.
15. In the Folder text box, enter the server name and share name to which you want to map the selected drive letter, and click **Finish**. Use the syntax: \\server name\share name. The figure below shows that you want to map drive L: on the local machine to a directory named Buried on the root directory of a remote system named CCI-HPAMD.




16. If necessary, enter your logon ID and password to access the server.
17. In Windows Explorer, click the mapped drive letter to see the contents of the Buried directory on the server.

Now copy a sample text file onto the server and make it available offline.

18. Copy the file **Treasure.txt** that was created in the preceding exercise, to the Buried directory on the server.
19. Right-click the *Treasure.txt* file on the server, and click **Always available offline**.

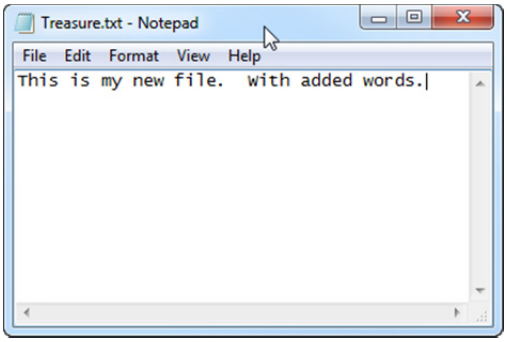
Shut down the server and make changes to your local copy of the Treasure.txt file.

20. **Server**: Shut down the server so that it is turned off.
21. **Computer**: Right-click the Treasure.txt file on your local machine and click **Edit** to open it in Notepad (or WordPad).
22. Add more words of your choosing to the file, then save and close it.

Notice that the left pane in Windows Explorer indicates that the mapped drive is offline.

23. **Server**: Power up the server again and log on to it.
24. Open Windows Explorer on the server and open the *Treasure.txt* file in C:\Buried to confirm that this version of the file does not contain the newly added text. Close the file.
25. **Computer**: Click the mapped network drive to access the Buried directory on the server, then click the Treasure.txt file on the server to select it.
26. Click the drop-down button next to **Sync** in the Windows Explorer menu bar, and click **Sync offline files in this folder**.
27. **Server**: On the server, open the *Treasure.txt* file in C:\Buried.

    The file on the server is now synchronized with the updates you made to the file on the local machine while the server was offline.

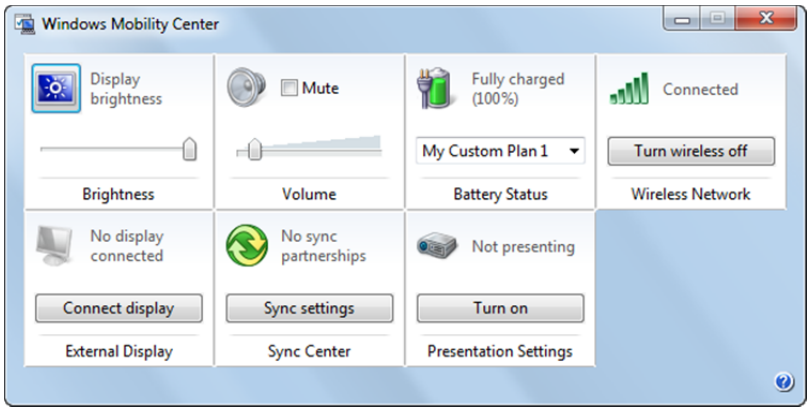



28. Close the *Treasure.txt* file on the server.
29. **Computer**: If desired, right-click the mapped drive on your computer and click **Disconnect** to remove the connection, and click **Yes** if a warning message is displayed (be sure that you closed the *Treasure.txt* file before doing so).

In this exercise, you practiced making a file available offline, making changes to that file while the server was offline, and synchronizing files when the server was online again.

## Windows Mobility Center

You use the Windows Mobility Center to configure settings (such as speaker volume, network connections, volume control) for mobile PC's such as a laptops or notebooks. While all of these options can be accessed using the Control Panel, the Windows Mobility Center enables you to modify all these settings from one central location.



Each square in the interface is called a tile and each tile contains one piece of information about a particular system component, as well as action items related to that component. You can click an icon on a tile to quickly open options for related setting. For example, you can click the battery icon to open the Power Options dialog box. The tiles that appear depend on the system.

Not all settings are available on all laptops. If a setting does not appear it may be because the required hardware is missing or turned off. For example, if you are not connected to a wireless network and the Turn wireless on button is not available, it could be because your laptop does not include a wireless network adapter, or it could be because the wireless network adapter is turned off.

You can access the Windows Mobility Center through the Control Panel, or in the Accessories folder on the Start menu. It is not accessible on non-mobile computers.

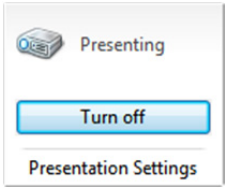
You can use the Windows Mobility Center to view and control the following features:

| | |
|---|---|
| **Brightness** | Adjusts the brightness of the screen. You can drag the slider to temporarily adjust the brightness, or you can click the icon to open the Power Plan options. |
| **Volume** | Adjusts the speaker volume. You can drag the slider to adjust the volume, or you can select the Mute checkbox. |
| **Battery Status** | Shows how much charge remains on the battery in your mobile PC. You can also select a power plan from the list. |
| **Wireless Network** | Shows the status of your wireless connection. You can also turn the wireless network adapter on or off. |
| **Screen Rotation** | Changes the orientation of your Tablet PC screen from portrait to landscape or vice versa. (Available on Tablet PCs.) |
| **External Display** | Allows you to connect an additional monitor to your mobile PC or customize the display settings. |
| **Sync Center** | Shows the status of an in-progress file sync. You can also start a new sync, set up a sync partnership, or change your settings in the Sync Center. |
| **Presentation Settings** | Adjust settings such as speaker volume and Desktop background in preparation for delivering a presentation. You can also connect your laptop to a projector and then click Turn on to get the computer ready to display a presentation. For example, the laptop will not sleep and system notifications will be turned off. Presentation settings are not available in Windows 7 Home Premium; they are available in Windows 7 Professional, Ultimate and Enterprise editions. |

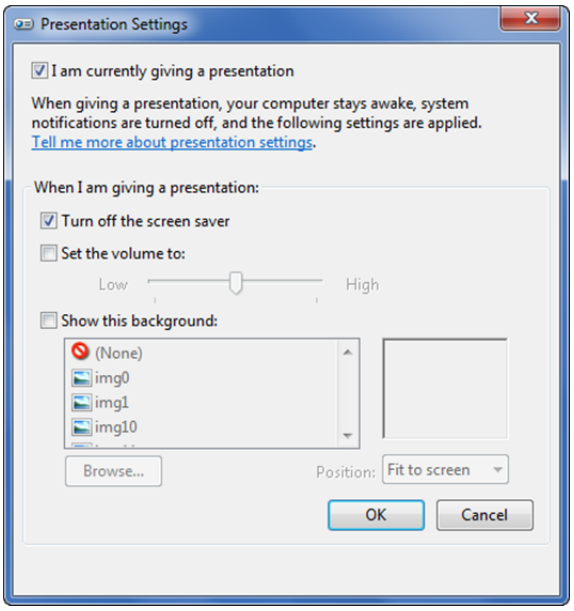
## Exercise 2-12: Using the Windows Mobility Center (Instructor-led)


In this exercise, your instructor will demonstrate how to use the Windows Mobility Center to prepare a laptop to deliver a presentation. This exercise requires the use of a portable PC such as a laptop or notebook computer.

1. Click the **Start** button, click **All Programs**, click **Accessories**, then click **Windows Mobility Center**.
2. In the Presentation Settings tile, click **Turn on**. Notice that the Presentation Settings have been enabled.




3. In the Presentation Settings tile, click the **Change presentation settings** icon to open the Presentation Settings dialog box. Notice that when you specify you are giving a presentation, the laptop will not enter sleep mode, and the system notifications are turned off. By default the screen saver is turned off as well. These settings ensure that your presentation will not be interrupted by events that occur on your computer.




4. Select the **Set the volume to** check box, then drag the slider to **High**. If your presentation includes audio, you can ensure that the audience can hear the audio file.
5. Select the **Show this background check box**, then scroll the images and select one that you like.
6. Click **OK** to apply the settings. Notice that the selected background displays on the Desktop.
7. If you have access to a projector, connect it to the laptop and then in the Mobility Center, click **Connect Display** in the External Display tile and configure an appropriate setting. If no projector is available, skip to Step 8.
8. Access the Windows Mobility Center again, and in the Presentation Settings tile click **Turn off** to return the laptop settings to their original values.
9. Close the Windows Mobility Center.

In this exercise, your instructor demonstrated how to use the Windows Mobility Center to prepare a laptop to deliver a presentation.

# Lesson Summary

In this lesson, you learned to configure various operating system components and features including Control Panel options and Desktop settings. You also learned about native applications and tools, and learned how Windows supports mobility. You are now able to:

- ☑ Identify the features and components of the Windows 7 Desktop.
- ☑ Understand how to navigate a breadcrumb trail.
- ☑ Identify the features and components of the Windows Explorer window.
- ☑ Add and configure Desktop gadgets.
- ☑ Describe and access user profile folders.
- ☑ Configure display settings, including screen resolution and screen magnification and configure Windows 7 to support multiple display devices.
- ☑ Create and modify Desktop shortcuts, create Start menu shortcuts, and add system icon to the Desktop.
- ☑ Use Aero features for window management.
- ☑ Modify and apply Aero themes.
- ☑ Use the Snipping Tool.
- ☑ Describe the major features of Internet Explorer.
- ☑ Describe the Windows Media Center.
- ☑ Describe Windows Media Player.
- ☑ Configure administrative tools.
- ☑ Configure accessibility options.
- ☑ Describe how to use MSCONFIG.
- ☑ Explain the Windows Sync Center.
- ☑ Explain the Windows Mobility Center.

**MMM**
Go online for Additional Review and Case Scenarios

# Review Questions

1. In which of the following situations might it be preferable to change screen magnification instead of screen resolution?
   a. When the monitor is a flat panel
   b When more than one user uses the system
   c. When the monitor is a CRT
   d. When a user is an administrator

2. Dean is using the System Configuration (MSCONFIG) utility on a Windows 7 system. What he is most likely trying to do?
   a. Troubleshoot a bootup issue
   b Configure accessibility options for a disabled user
   c. Change the appearance of the Desktop
   d. Synchronize offline files with files in a network share

3. Ken is viewing the user profile folders on his Windows 7 system. Which tool is he using?
   a. MSCONFIG
   b Computer Management Console
   c. Windows Explorer
   d. Registry Editor

4. Which Aero feature can you use to make all open windows transparent?
   a. Aero Peek
   b Aero Snap
   c. Aero Invisible
   d. Aero Shake

5. Which Internet Explorer feature is designed to help users avoid known phishing Web sites?
   a. InPrivate Browsing
   b SmartScreen Filter
   c. the Internet security zone
   d. Internet Explorer accelerators

# Lesson 3: Managing Users and Applications

## Lesson Objectives

In this lesson, you will explore some of the tools and features that allow an administrator to manage users and computers. By the completion of this lesson, you will be able to:

- ☐ Explain administrator and standard user accounts.
- ☐ Describe the function of the User Account Control feature and describe its prompts and elevation levels.
- ☐ Describe the process of local, network, and group policy application installation.
- ☐ Install and remove application software.
- ☐ Describe the function and characteristics of services, and identify startup types, service accounts and service dependencies.
- ☐ Describe the advantages provided by remote management tools.
- ☐ Explain the Microsoft Management Console (MMC) and create a custom console.
- ☐ Explain how group policy is useful for remote management.
- ☐ Describe Windows PowerShell.
- ☐ Describe the function of Remote Desktop and explain the necessary configuration settings and underlying technologies.
- ☐ Explain application virtualization and describe the features and functions of App-V, Remote Desktop Services, and RemoteApp.
- ☐ Explain Virtual Desktop Infrastructure (VDI).

### Exam Objectives

1.4 Understand mobility
1.5 Understand remote management and assistance
2.4 Understand virtualized clients
3.1 Understand application installations
3.2 Understand user account control (UAC)
3.4 Understand services
3.5 Understand application virtualization

## Managing Windows

Throughout your career as an IT professional, you will perform tasks related to the management of hardware, software, and users. The term management can apply to setting up and configuring systems for end-user use, installing, configuring or removing applications, controlling which particular features will be accessible to users, or controlling which user has access to which resources.

Windows provides a wide variety of tools and features that allow you to configure and manage both local and remote Windows computers. In this lesson, you will explore several of these tools and features.

In computing, there are local machines and remote machines. For example, consider that Ed and Ron work in the same office and that each has his own computer. The computer that Ed logs on to and sits in front of is his local machine. Additionally, the computer that Ron logs on to and sits in front of is Ron's local machine, but to Ed, Ron's computer would be a remote machine because it is not at his immediate location.

# User Accounts

Objective 3.2

You learned in Lesson 1 that there are three different types of user accounts in Windows 7: standard user accounts, administrator accounts, and a guest account. (The guest account is created during operating system installation and is turned off by default.)

Each type of account has a specific level of permission associated with it. *Permissions* are rules associated with objects on a computer, such as files, folders and settings. Permissions determine whether you can access an object and what you can do with it. Creating and using the appropriate types of user accounts provide a first step in managing a Windows system.

The two account types you deal with most often on a Windows 7 system are:

| | |
|---|---|
| **Administrator account** | Lets you make changes to the system that will affect other users. Administrators can change security settings, install and uninstall software and hardware, and create or make changes to other user accounts on the system. When Windows 7 is installed, it automatically creates an administrator account. You use this account to install programs, configure the system and create and change other user accounts. |
| **Standard user account** | Lets you use most of the capabilities of the computer. You can use most programs that are installed on the computer and change settings that affect your user account. However, you can't install or uninstall some software and hardware, you can't delete files that are required for the computer to work, you can't access files stored in other users' profile folders, and you can't change settings that affect other users or the security of the computer. |

The guest account has very limited permissions. People using the guest account have limited access and cannot change settings, install hardware or software or create a password.

## Controlling Access to Resources

One of the basic goals of an IT professional is to protect and secure the resources of an enterprise. From a security standpoint, the primary rule is to provide the least amount of access privileges required for users to perform their daily tasks. It is therefore important to understand each job function and assign permissions and account types accordingly. For example, a user in data entry who spends all day entering customer orders into the enterprise database does not require access to the enterprise Web server, except perhaps to request Web pages on the company intranet. The Web server administrator on the other hand, requires access to the Web server, but does not require access to confidential documents handled by the Human Resources department.

Assigning suitable access to employees accomplishes the following:

- **It prevents intentional damage or breach of security** – some users intentionally create security holes or sell confidential information. Therefore, the fewer people who have power to create breaches or access confidential information, the better.
- **It prevents accidental damage or breach of security** – some users unwittingly create security holes or perhaps have copied confidential files from a network share to their local machine without knowing what those files contained. If these users' systems are compromised, there could be a resulting leak of information or illicit access into the network. Again, the fewer people who have power to create breaches or access confidential information, the better.
- **It provides a layer of protection against malware and hackers** – arguably, the biggest danger of working with privileges and permissions that exceed those of your job requirement is that if your account is hacked or hijacked, the hijacker exerts the same level of permission as you do over the system. For example, if a hacker is able to illicitly log on using a standard user account, he or she could destroy files to which that user had access, but could not make system-wide changes or disable security, or delete accounts. On the other hand, if a hacker is able to illicitly log on using an administrator account, he or she could lock other users out of the system, disable the firewall, and do considerable damage.

## Working as a Standard User

An administrator account is created when you install Windows 7 so that you can install other hardware and software, configure the system and security settings, and create other user accounts if required. If you are the only person using the computer, it might seem like a good idea to simply continue using the administrator account. However, it is considered best practice to create a standard user account and to use the standard user account to perform your day-to-day computing tasks.

When you use a standard user account, you will be prompted to enter an administrator password before you can perform certain tasks, such as changing the security settings or updating device drivers. Prompting you to enter a password is Windows' way of bringing to your attention the fact that you are about to make a significant change to the system. The logic behind prompting you is two-fold:

- it gives you a moment to stop and think, and may prevent you from making unintentional changes
- it alerts you that a process or program is trying to make changes to the system. (This is important because some malicious programs attempt to install software or make system changes without your knowledge.)

In previous versions of Windows, it was inconvenient to work as a standard user because every time you needed to make substantial configuration changes, or wanted to install software or drivers, you had to log off as the standard user and then log on as an administrator in order to perform the desired tasks.

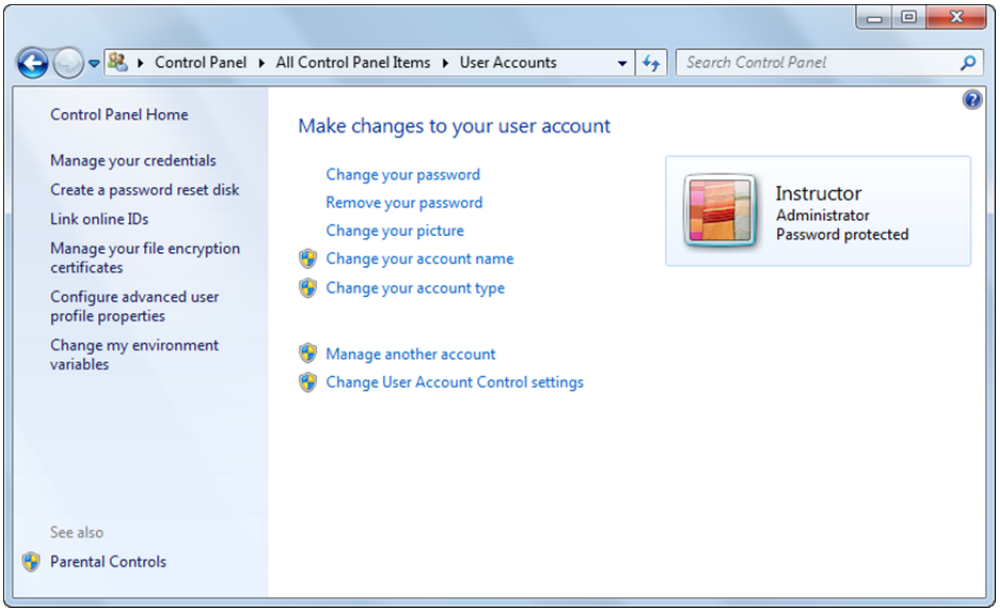
In Windows 7, user account control (UAC) adjusts permission levels so that you have permissions appropriate to the tasks you are performing. This means you can log on as a standard user, and when you want to perform tasks that require administrator-level permissions, Windows 7 will prompt you for your credentials and you can proceed. You no longer need to log off, and log back on as an administrator.

## Exercise 3-1: Creating a New Standard User Account


In this exercise, you will create, use and then delete a standard user account.

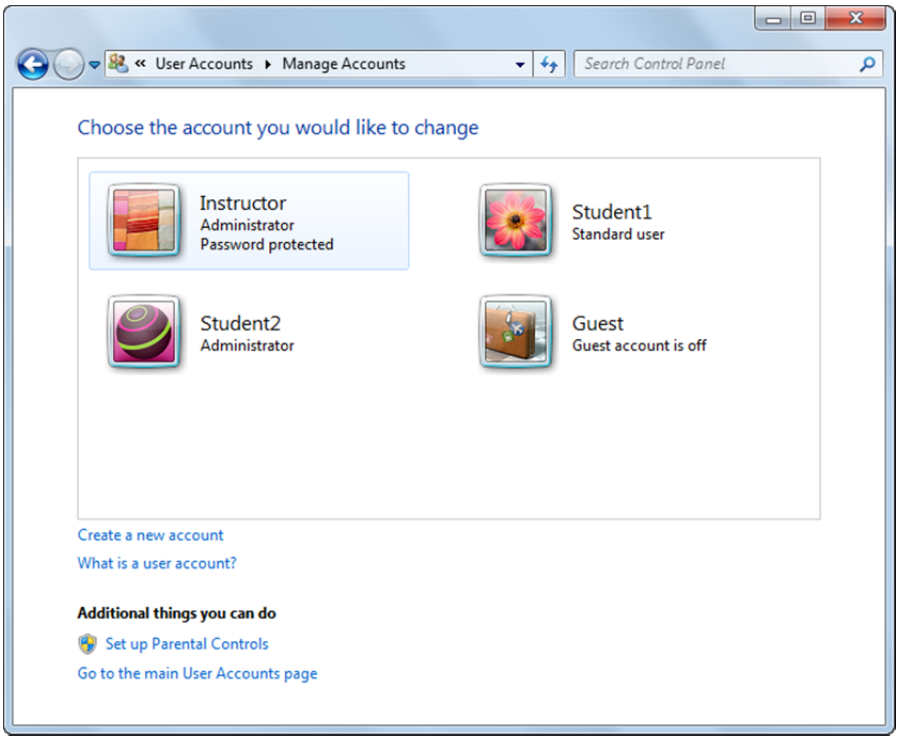
First, you will create a new standard user account.

1. If necessary, log on to your computer with an administrator account. You must be logged on as an administrator in order to create an account.
2. Click the **Start** button, click **Control Panel**, if necessary, display the View by drop-down list and select either Large or Small icons, then click **User Accounts** to open the User Accounts page of the Control Panel.

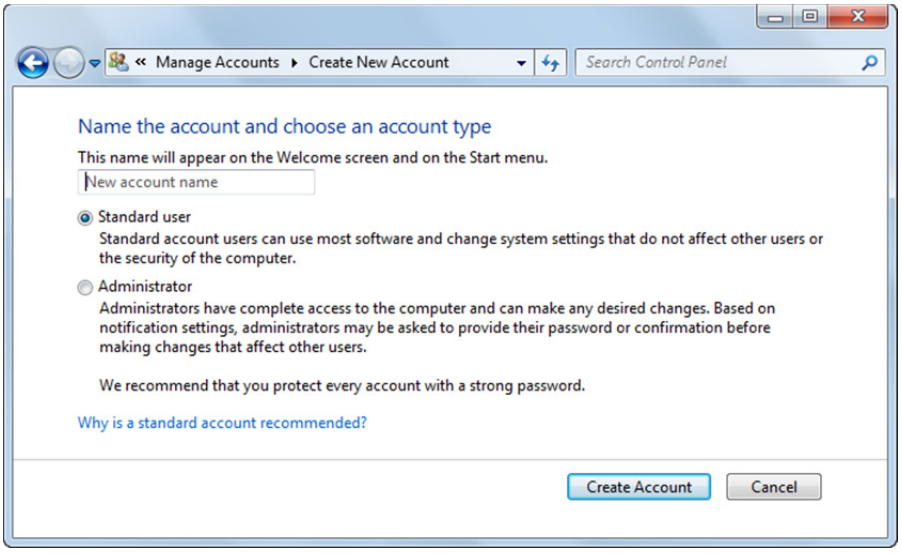



You can perform several account maintenance tasks from the User Accounts page, including changing your account picture or password, or removing your password. When you are logged on as an administrator, you can also change your account name, your account type, the user account control settings, or manage accounts other than your own.

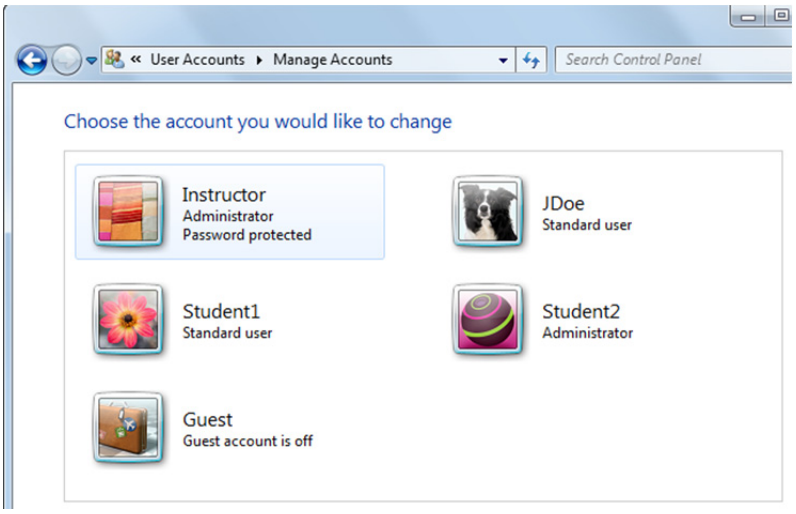
3. Click **Manage another account** to open the Manage Accounts page. From this page, you can manage any account on the system, turn the Guest account on or off, or create a new account.



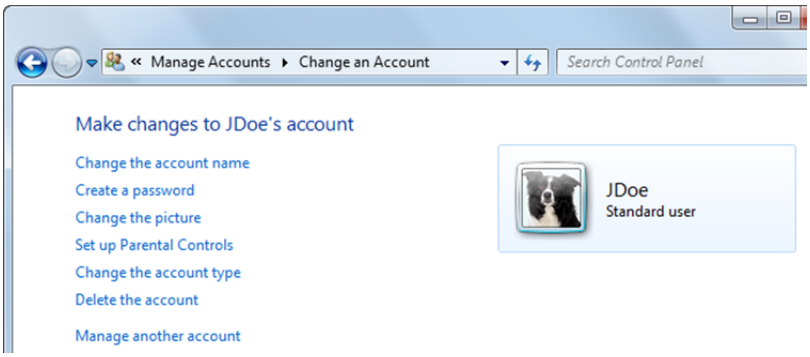

4. Click **Create a new account** to open the Create New Account page. Notice that you can create either a standard user account or an administrator account.



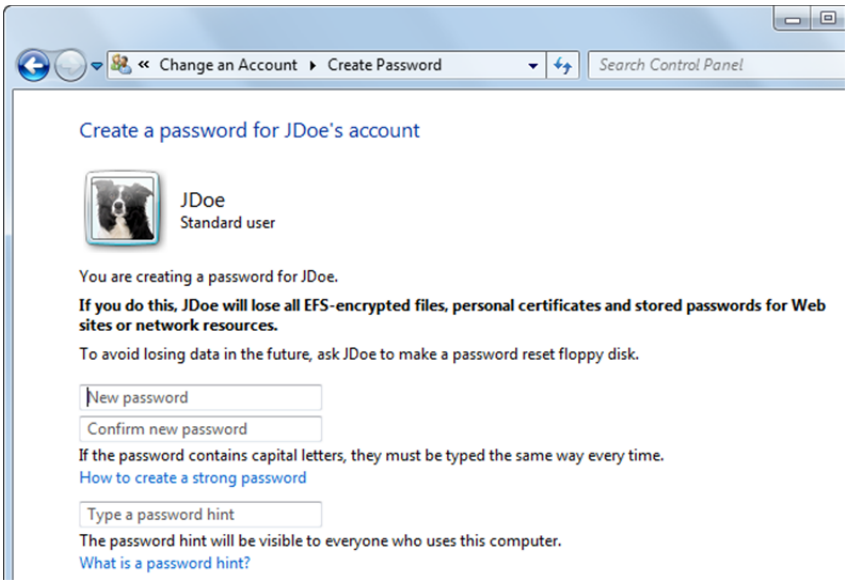

5. Type: JDoe in the New account name box, ensure that Standard user is selected and click the **Create Account** button to create the new standard user account. Windows creates the account and lists it in the Manage Accounts page. You can now manage various features of the account.




6. Click the **JDoe Standard user** account to view the available management options.




7. Click the **Create a password** link to open the Create Password page.

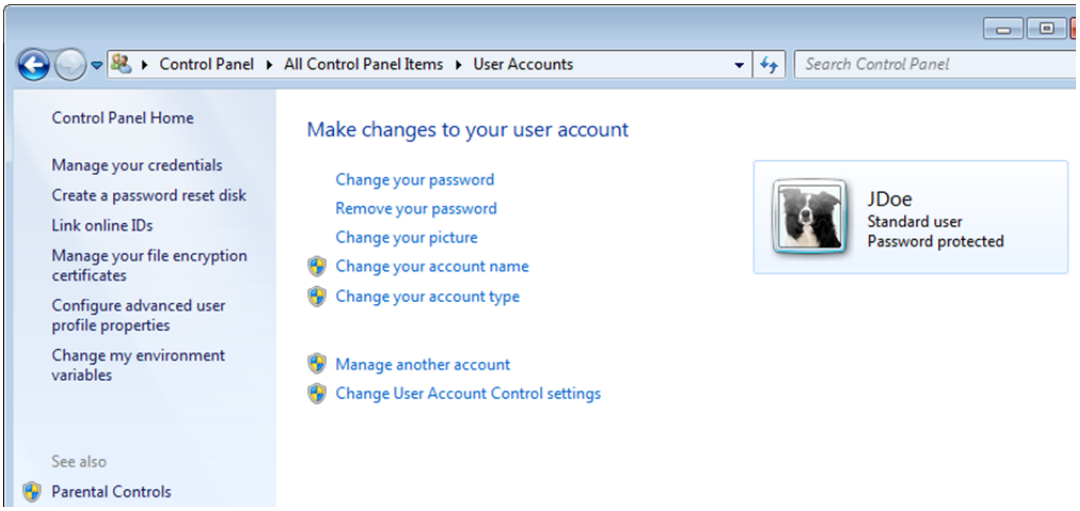



Notice the warning concerning losing access to EFS-encrypted files, personal certificates and stored passwords. This warning does not apply when you are first creating a user account, nor does it apply when a user logs in and changes his or her own password or first adds one to the account. The typical case where this warning applies is when a user has forgotten his or her password and an administrator must create a new one.

8. Type: anon in the New password box, press TAB, then type: anon in the Confirm new password box. (This is not an example of a strong password and is used here for the sake of simplicity.) When you have entered the new password twice, click **Create password** to add the password to the account.

Next, you will log off as administrator and log on as the new standard user.

9. Close the Control Panel.
10. Click the **Start** button, display the Shut down options, then click **Log off**.
11. On the Windows 7 login screen, click **JDoe**, type: anon in the Password box, then press ENTER to log on using the new standard user account. It may take a few moments for Windows to prepare the new user profile and Desktop.
12. When you are logged in, click the **Start** button, click **Control Panel**, display the View by drop-down list and select either Large or Small icons, then click **User Accounts** to open the User Accounts page of the Control Panel.




Notice that the options presented here are slightly different than the ones presented to the administrator account in Step 6. The last four items include a User Account Control (UAC) symbol, indicating that an administrator password must be entered to access that particular option. (You will learn about the UAC in the next section.)

13. Click **Change your password** to open the Change Your Password page. You can change your password as often as necessary as long as you can correctly enter the current password.
14. Click the **Back** button at the top of the window, then click **Remove your password** to open the Remove Your Password page. Again, you can remove your password as long as you can correctly enter the current password.
15. Click **Cancel**.
16. Click **Change your picture**, click a picture in the gallery, then click the **Change Picture** button.
17. Click the **Start** button. Notice that the new account picture displays above your user name in the Start menu.
18. Press Esc to close the Start menu.
19. Click one of the remaining options. You are prompted to type an administrator password and then click Yes before Windows will allow the Control Panel to make changes to the computer.
20. Click **No**.

Next, you will log back on as administrator and delete the new standard user account.

21. Close the Control Panel, click the **Start** button, display the Shut down options, then click **Log off** to log off the standard user account.
22. Log back in using your administrator account.
23. Open the Control Panel, then open the User Accounts page.
24. Click **Manage another account**, then click **JDoe Standard user Password protected**.

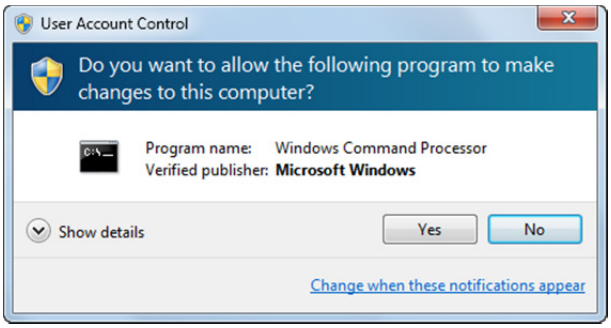
25. Click **Delete the account**, click the **Delete Files** button, then click **Delete Account** to confirm that you want to delete the standard user account you created. When you specify to delete files, these are the contents of the user Desktop, Documents, Favorites, Music, Pictures and Video folders. If you specify to keep the files, Windows will copy them to a folder on your Desktop. The folder is named with the user account.
26. Close the Control Panel.

In this exercise, you created, used and deleted a standard user account.

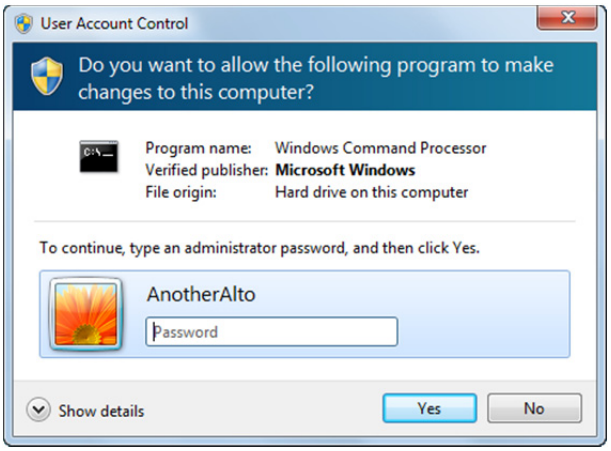
# User Account Control (UAC)

User Account Control (UAC) is a feature in Windows that issues notices (called elevation prompts) when a program is about to make a change that requires administrator-level permission. For example, when you or programs you are using need to make changes that require administrator-level permission, UAC presents an elevation prompt and gives you options for proceeding:

- If you are logged on as an administrator, you can click Yes to continue




- If you are logged on as a standard user, you (or someone else with an administrator account on the system) must select the administrator account presented in a dialog box and enter the administrator password.




If you click Yes, or enter the administrator password, your permission level is temporarily elevated to allow you to complete the task, then your permission level is returned to that of a standard user.

UAC works by adjusting the permission level of your user account. If you are performing tasks that can be accomplished as a standard user (such as reading email, or creating documents), you have the permissions of a standard user, even if you are logged on as an administrator.

Because UAC issues a notification regardless of which type of account you have used to log on, you are always made aware when a program is about to make a change that requires administrator-level permission. This notification process can therefore prevent malicious software and spyware from being installed or making changes to the system without your knowledge.

UAC presents four different types of notification dialog boxes, depending on who published the item that needs permission to continue. Windows can tell who published an item by checking its digital signature. A digital signature is an electronic security mark that can be added to a file. It allows you to verify the publisher of a file and helps verify that the file has not changed since it was digitally signed. The UAC notification dialog boxes are outlined in the following table:

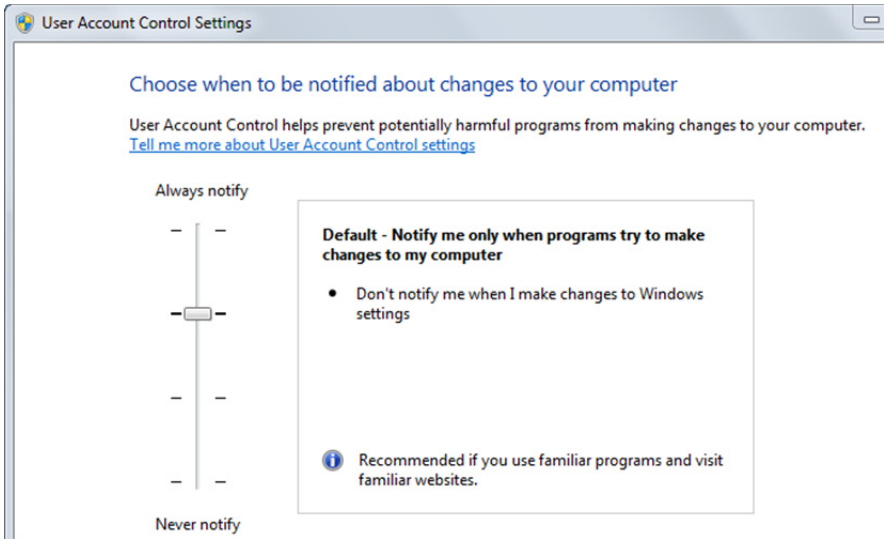
| Icon | Type | Description |
|---|---|---|
|  | A setting or feature that is part of Windows needs permission. | Microsoft is the publisher of the item. |
|  | A program that is not part of Windows needs your permission to start. | The program has a valid digital signature, but Microsoft is not the publisher. |
|  | A program with an unknown publisher needs your permission to start. | The program does not have a valid digital signature from its publisher. This does not necessarily imply that the program is unsafe; simply that it is unsigned. Be sure that you obtained the file from a trusted source. |
|  | You have been blocked by the system administrator from running this program. | The program has been blocked because it is known to be untrusted. You cannot proceed. If you need to run the program, you must contact the system administrator. |

When you are notified, your Desktop is dimmed and you must either approve or deny the request in the UAC dialog box before you can do anything else on the computer. The dimming of the Desktop is referred to as the secure desktop because no programs can run while the Desktop is dimmed. You can, however, configure UAC not to dim the Desktop.

## Configuring UAC

Some users feel that UAC issues too many notifications; others want to know about every change made to the system. As an IT administrator, you must consider company policy and configure the systems accordingly. You can configure UAC to provide notifications that suit your needs and preferences.

Configuration adjustments can be made using the User Account Control Settings dialog box in the Control Panel.

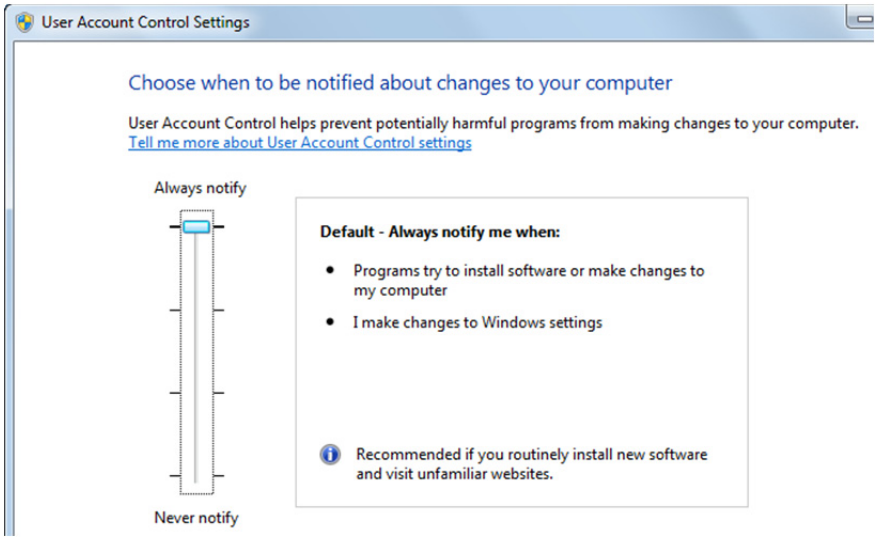


Drag the slider to one of the four positions described below.

| Setting | Description | Security impact |
|---|---|---|
| Always notify | You will be notified before programs make changes to the system or to Windows settings that require administrator-level permissions. | This is the most secure setting. |
| Notify me only when programs try to make changes to my computer | You will be notified before programs make changes to the system.<br>You will not be notified if you try to make changes to Windows settings that require administrator-level permissions.<br>You will be notified if a program outside of Windows tries to make changes to a Windows setting. | This is the default setting. You are advised to be careful about which programs you allow to run on your computer. |
| Notify me only when programs try to make changes to my computer (do not dim my desktop) | You will be notified before programs make changes to the system.<br>You will not be notified if you try to make changes to Windows settings that require administrator-level permissions.<br>You will be notified if a program outside of Windows tries to make changes to a Windows setting. | Essentially the same as "Notify me only when programs try to make changes to my computer," but you are not notified on the secure desktop. |
| Never notify | You will not be notified before any changes are made to your computer. If you are logged on as an administrator, programs can make changes to your computer without your knowing about it.<br>If you are logged on as a standard user, any changes that required administrator-level permissions will be automatically denied.<br>Requires a restart to complete the process of turning off UAC. Once UAC is turned off, people that log on as administrator will always have the permissions of an administrator. | Turns off UAC.<br>This is the least secure setting and is not recommended. |

You must be logged on as an administrator in order to modify UAC settings.

If you are logged on using a standard user account, you will be prompted to enter the administrator password when you try to modify the UAC settings. Upon entry, the UAC Settings screen will offer a slightly different set of options:



## Exercise 3-2: Examing UAC Settings


In this exercise, you will explore various settings for UAC.

1. If necessary, log in using an administrator account.
2. Click the **Start** button, then click **Control Panel** to open the Control Panel window.
3. Switch to either Large or Small icons view if necessary, then click the **User Accounts** link.
4. In the User Accounts screen, click the **Change User Account Control settings** link to open the User Account Control Settings dialog box.
5. What is the current setting? For which situations is this setting recommended?
6. Drag the slider up to the **Always notify** setting. Notice that this setting is recommended if you routinely install software and visit unfamiliar Web sites. Why do you think this setting is appropriate for these conditions?
7. Drag the slider down to the **Notify me only when programs try to make changes to my computer (do not dim my desktop)** setting. Notice that this setting is not recommended. What extra level of protection is provided through dimming the desktop?
8. Drag the slider down to the **Never notify** setting. Notice that this setting is not recommended, and is suggested only for cases where you must use software that is not compatible with User Account Control.
9. Click **Cancel** to close the User Account Control Settings dialog box without saving any changes.
10. Close any open Control Panel dialog boxes.

In this exercise, you examined various settings for UAC.

# Installing and Uninstalling Applications

Objective 3.1

As you already know, the operating system controls all hardware and application software on the computer. Application software, such as word processing programs, database programs, or spreadsheet programs make the computer useful and enable the user to be productive.

You can install application software using the following methods:

- Local installation
- Network installation
- Group policy

## Local Application Installation

A local application is installed and runs on the local machine. Local applications are the programs that appear in the Start menu and/or can be accessed by shortcuts on the Desktop or in the taskbar. Accordingly, local application installation is performed while sitting at the local machine. In order to locally install an application, you must have:

- Administrator-level permissions on the system
- Access to the installation media (DVD, CD, USB), or access to a downloaded executable file that you can use to install the application

Most applications are packaged with an AutoRun feature that will start the installation as soon as you insert the removable media. You simply insert the disc, wait for the setup program to start, and then follow the instructions.

In cases where you are using an executable file, you simply double-click the file to begin the process. Note that if you download software from the Internet, it is considered best practice to save the installation files and scan them for viruses before installing. Software from a reputable vendor will rarely have problems; however, if you download software from a site that is not the vendor's official Web site, spyware or viruses could be embedded in the download file.

If an application installation does not begin automatically, you can use Windows Explorer to search for the setup program, which is usually named Setup.exe or Install.exe.

If the media does not contain a Setup.exe or Install.exe file, you can look for a file named README.txt. These files often contain installation and configuration instructions and release notes.

In most cases, these installations are interactive. When performing a local installation, you are most commonly asked to specify:

- the name of the user
- a product ID key or serial number
- an installation location (if different than the suggested default location)
- whether the application should be made available for all users on the system or only for the current user.

## Installation Engine

Most application setup programs make use of the Windows Installer engine. Windows Installer is an installation and application configuration service that runs on Windows operating systems. When application setup programs use Windows Installer, the installation information and the installation files are contained in installation packages known as MSI files. These files can also be launched directly by double-clicking them.

MSI files rely on Windows Installer to copy files, create folders and create registry entries during the installation process. The Windows registry is a database that stores configuration settings and other options on Windows machines. All installed programs are represented by entries known as keys in the registry. (You will learn more about the registry in a later lesson.) Registry keys for uninstalling the application are also created at this time.

Some applications use a custom-coded installation engine, which manually copies files and configures registry entries.

## Default Installation Locations

Application software installation programs are geared to install program files in a default installation location. In many cases, you are given the opportunity to specify an alternate location. In most cases, it is best to accept the suggested default location; if you specify an alternate, you may be forced to remember and specify the appropriate path to the program files when performing configuration, repair, or uninstallation tasks.

While each program will create its own folders and subfolders, the general default installation locations on a Windows 7 system are as follows:

- On 64-bit systems
  - 32-bit applications are stored in C:\Program Files (x86)
  - 64-bit applications are stored in C:\Program Files
- On 32-bit systems, 32-bit applications are stored in C:\Program Files (64-bit applications cannot be installed)

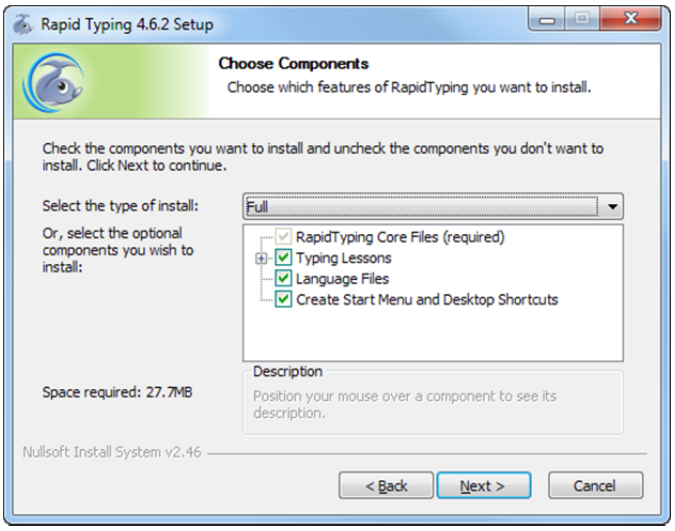
# Exercise 3-3: Installing an Application


In this exercise, you will install an application. The program used in this exercise was selected because it is representative of many applications and demonstrates the standard installation process. This exercise should not be considered an endorsement or recommendation for any program.

1. In the student data folder on the desktop, navigate to the *Lesson03* folder and then double-click the *RapidTyping_Setup_4* file.
2. If you are logged on using a standard user account, enter the administrator password and press ENTER. If you are logged on using an administrator account, click **Yes** if the UAC appears.
3. Click **Next**.

Always read the full license to be certain of your rights and what you can do with the program.

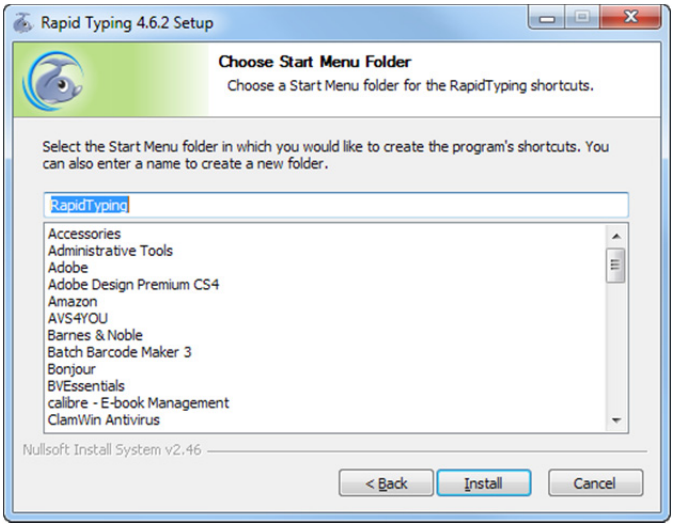
4. Read the license agreement and then click **I Agree**.
5. Click **Next** to accept the default installation location.




You may be given the opportunity to select particular components to include in the installation. Explore the options carefully. For instance, if the only language you plan to use is English, you may not want to install all the different language files.

6. Expand the Typing Lessons tree by clicking on the **+** icon, then select which courses you want to install by either selecting or clearing the appropriate check boxes, then click **Next**.

   Sometimes you are asked to specify in which Start Menu folder you want to create the program's shortcut.



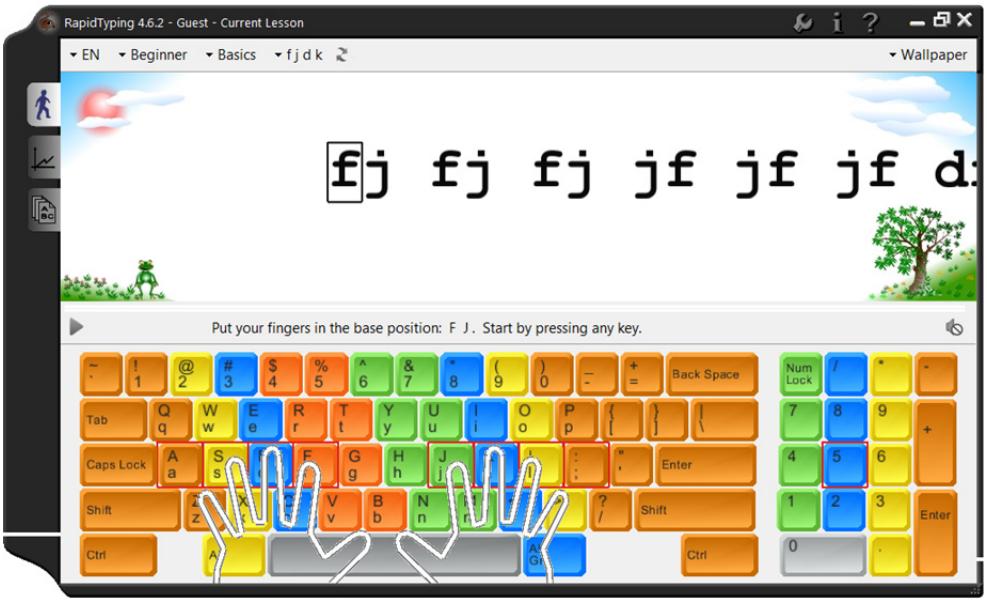

7. Click **Install** to begin the installation.
8. When the Completing the RapidTyping Setup Wizard screen appears, clear the **Check the latest version at rapidtyping.com** check box, then click **Finish**.

   The wizard completes the installation and should place a shortcut on the Desktop (unless you opted to not have the program create a shortcut).

9. To start the program, double-click the **RapidTyping** icon on the Desktop. Alternately, you can click **Start**, **All Programs**, **RapidTyping**, **RapidTyping**.

Depending on which check boxes you selected or cleared during the installation, you may be able to select from several different languages when you first open the program.

10. Select the language you want to use (this exercise uses English) and click **Next**.
11. Select the correct (or the closest) keyboard type for your system and click **Finish**.




The installation is now complete and the program is ready to use.

12. Click the close button to exit the program.

In this exercise, you installed a local application.

## Configuring Local Applications

While in most cases, application software is configurable through the application interface itself, some programs allow you to add or remove features through the Control Panel. For example, you can add or remove available components of Microsoft Office in the Control Panel.

If an application is configurable in this manner, you will see a Change button in the Programs and Features Control Panel.

## Uninstalling

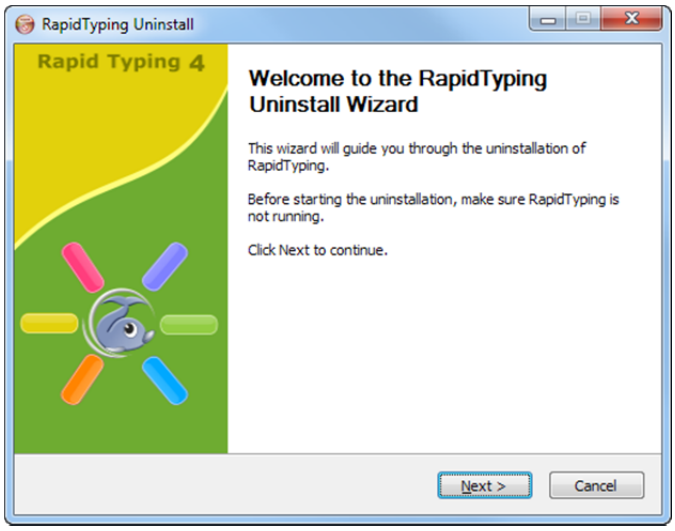
When you install a program, configuration information is added to the Windows registry so the operating system will identify the installed program. If you try to remove a program by simply deleting its files using Windows Explorer, the obsolete configuration information is left in the registry.

To properly remove a program, uninstall it using the Programs and Features Control Panel. Display the installed programs, then in the list box, select the program you want to remove and click the **Uninstall** or **Uninstall/Change** button that appears in the command bar at the top of the list box.

## Exercise 3-4: Uninstalling an Application


In this exercise, you will uninstall an application.

1. Click **Start**, **Control Panel**, **Programs and Features**.
2. Scroll in the list box and select the **RapidTyping** program. Then on the command bar, click **Uninstall**.
3. If you are logged on using a standard user account, enter the administrator password.




4. Click **Next**.
5. Confirm the location where this program was installed (if you changed the default installation location when you installed the program, you will need to confirm that location is accurately displayed before proceeding) and click **Uninstall**.
6. Click **Finish**.

   The program no longer appears in the list box in the Control Panel window.
7. Close the Control Panel window.

In this exercise, you uninstalled a program.

### Custom Uninstall Routine

In some cases, such as when an application was installed using a custom-coded installation engine, the application will not appear in the Programs and Features Control Panel list box. The application may include a custom uninstallation engine – look in the Start menu to see if an uninstaller for the application is available. You can also check the installation directory for an uninstall routine.

### Third-party Uninstallers

Sometimes you will not be able to find an uninstall routine for your application, or you may begin an uninstallation that halts because configuration files are damaged or missing. In such cases, you may be able to use a third-party uninstaller. These applications are used to uninstall applications and remove traces from programs that did not uninstall correctly.

Third-party uninstallers are also useful for cleaning up programs that did not install correctly in the first place, and subsequently will not uninstall.

### Manually Removing an Application

If you are unable to successfully locate or run an uninstallation routine, you will have to manually remove an application. To do so, you must:

1. Delete all shortcuts to the application, including any Start menu folders that may have been created.
2. Delete all files in the application folder and then delete the folder itself.
3. Delete registry entries that refer to the application.

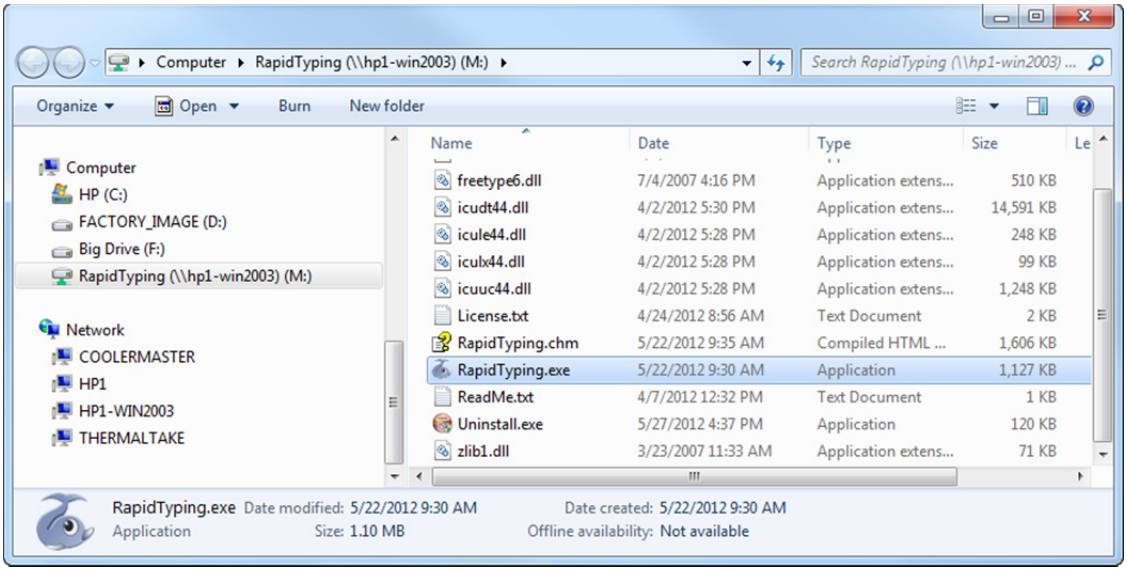
If you must manually remove an application, you should proceed with caution. Applications often share files, and it is possible to inadvertently delete files that are needed by another application. Also great care must be taken when editing or deleting items from the registry.

# Network Application Installation

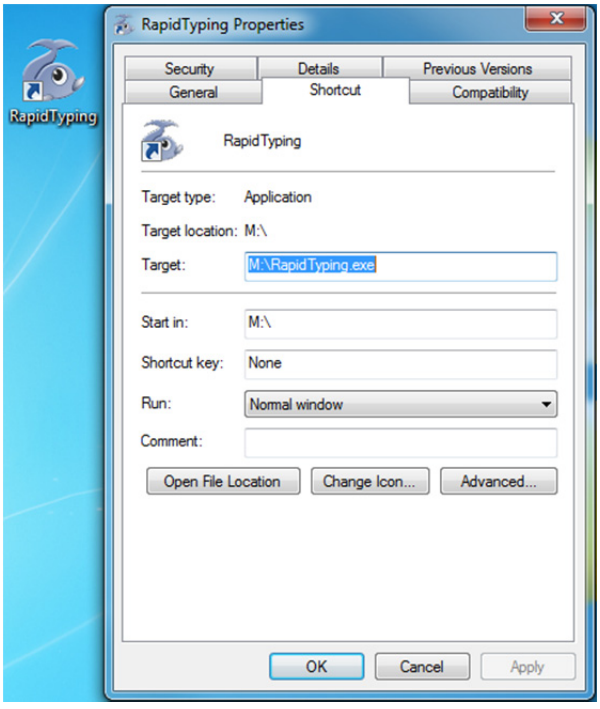
Instead of installing an application locally, you can also install it on a remote computer (usually a server) and configure other computers on the same network to run it from that server. When a user starts up the application, the local computer accesses and runs the executable (EXE) file from the remote server. Even though the program file is stored elsewhere, the program starts up and runs as if it were installed locally; it will continue using resources on the local computer such as RAM, CPU, hard drive, and other devices. The main advantage of this configuration is the ease of upgrading the application software – it needs to be done only once on the remote server instead of on every computer.

Once the software has been installed on the remote server, each local computer must be configured to access it:

- The folder where the application is stored on the remote server must be mapped to a local drive letter.




- A shortcut must be added to the Start/All Programs menu and/or the Desktop to allow users to access the application. This shortcut must use the mapped drive described above.




- If necessary, add any registry settings to the local computer required by the application.

The main disadvantage of running an application from a network server is that all computers depend on that remote server to be running whenever the software is needed. Servers are designed to run continuously (they are generally shut down only for maintenance); however, in a very small office environment you may not have any servers to perform this function. Therefore, if a desktop PC is designated to act as the application server for the group of networked computers, then that PC must be powered on at all times or be powered up first before the others.

Cloud-based applications are another form of networked applications. They are accessed by client systems using a web browser. In this configuration, the application is designed to run on remote servers that are typically offered by an external service provider. An interesting aspect of cloud-based applications is that no part of the application is downloaded to the local machine: the application software is designed to be used by any user at any location using any variety of computer that is capable of running a web browser and java applets, including PC, Mac, or Linux.

There are also other configurations that allow multiple users to share an application program including remote desktop connection and VDI. These are described in more detail later in this lesson.

## Installation through Group Policy

In an enterprise, Group Policy can be used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment. That is, Active Directory knows all of the authorized users and computers within an enterprise and how they are organized into groups or departments.

This capability allows you to use Group Policy to easily deliver and install application software or upgrades to targeted groups of users or computers. If you want to use Group Policy to deploy an application, the following conditions must be met:

- all the Windows clients must be members of an Active Directory Domain Services (AD DS) domain,
- you must use Windows Installer (MSI) files, and these files must be located on a network share that the user can access with at least read permissions, and
- you must create a Group Policy Object (GPO) in the AD DS domain to deploy the application.

When an application is deployed through Group Policy, it can be either published or assigned. When an application is published it is made available on the computer for installation from the Add or Remove Programs link in the Control Panel; the user must then select the option to actually perform the installation. When an application is assigned, it installs automatically the next time the user logs onto the machine and tries to use the application, or reboots the computer, depending on how the application is assigned.

Group Policy enables centralized management of software deployment, including uninstalling, upgrading or modifying software packages. The Group Policy can also be configured so that the software is removed when a user who does not have access rights logs on to the computer. Note that Group Policy does not perform software metering. In other words, you must ensure that you have purchased enough licenses to deploy these applications to the users; Group Policy does not count or verify that you have enough licenses for your enterprise.

You will take a closer look at Group Policy and the Local Group Policy Editor later in this lesson.

# Understanding Services

Objective 2.4 3.4

A *service* is nothing more than an application program that runs in the background. The unique characteristic of services is that they are designed to run without any direct interaction with users. Services are generally supplied by three types of providers: Microsoft, third-party hardware manufacturers and software developers, and in-house software developers.

The software with which you are most familiar requires some kind of user interaction. Specifically, you decide when to start and exit the software, and you enter various commands and data into the program as you use it. In contrast, a service does not have any interaction with the user, it starts automatically when the computer is powered up, stops automatically when the system shuts down, and is designed to communicate with other devices or systems. It is these characteristics that make them ideally suited for enterprises with many complex systems. For example, during a recovery from a power outage, system operators are usually very busy working through checklists to bring all systems back online. Services are exceptionally easy to handle – the operators simply ensure the server is successfully powered on; the services will automatically start up on their own and no one needs to log in to press a Start button, for example. This level of simplicity ensures that services become available as quickly as possible and avoids failures caused by human error. As a result, corporate in-house developers predominantly design software to run as services or other similar autonomously-run software on servers.

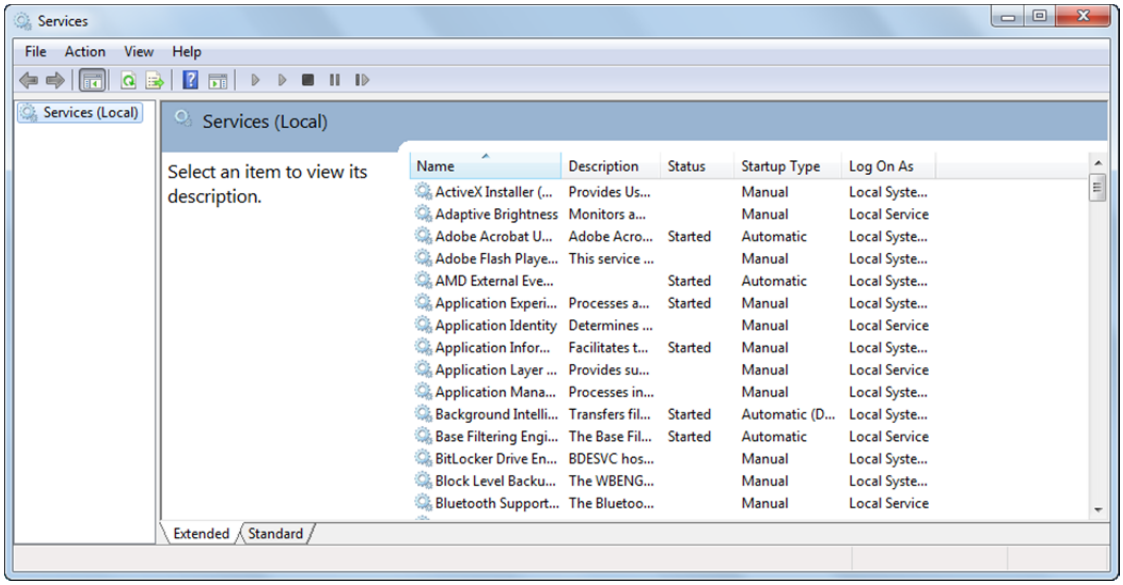
Microsoft also provides many services required to support core operating system features, such as Web serving, event logging, file serving, printing and error reporting.

Microsoft-developed services with which you may be familiar include:

| | |
|---|---|
| **Cryptographic services** | Provides for the management of digital certificates for authentication and encryption. |
| **DHCP client** | Allows a system to receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server on a network. Each system on a network needs an IP address. |
| **Encrypting File System (EFS)** | Provides file encryption technology used to store encrypted files on NTFS file system volumes. |
| **Netlogon** | Used to log into an Active Directory Domain Services domain. Without this service, you cannot join a machine to a domain. |
| **Print Spooler** | Provides local and network printing queues enabling a single printer to handle more print jobs than its internal memory would allow. If you want to share a printer on your machine, you must run this service. |
| **Remote Desktop Services** | Allows a user to connect to and manage a remote computer. |
| **Task Scheduler** | Monitors the system for scheduled tasks and executes them at the defined time. |
| **Windows Event Log** | This service logs (records) specific events that you can view with the Event Viewer. |
| **Windows Firewall** | Provides a software firewall to prevent unauthorized users from gaining access to the computer through the Internet or a network connection. |
| **Windows Update** | Enables the detection, download and installation of updates for Windows and other programs. |

Third-party software such as antivirus software are also designed as Windows services that run silently in the background, but generate pop-up messages to alert you when necessary. Hardware manufacturers may also supply services to be installed on your computer to work in conjunction with the equipment that you purchased. For example, a network scanner is designed to efficiently scan large volumes of paper documents into images. Because the scanner is not connected directly to any computer, there must be a method of transferring the images to the correct destination. If the software for performing this function is embedded into the hardware, it becomes more difficult and time-consuming to upgrade it. But if the manufacturer takes an alternate path by designing the software to run as a service under Windows, upgrades are easier and faster.

If you examine the list of services running on your computer, you will be surprised at how many there are. The particular services that are installed and running on a Windows machine varies from system to system based on the type of software and features that are installed. To view the services on a system, click **Start**, then type: `services.msc` in the Search field to open the Services snap-in. (A snap-in is a special type of administrative tool.)



The downside is that each running service consumes system resources and adds to system overhead, and each service may be in one of several states at any given time. These states include stopped, started, and paused. Notice that in the Services snap-in shown above, only certain services are running (Started). If your computer is experiencing very sluggish performance, you should review the running services; you may have installed some of them with devices or other software that you are no longer using.

You can also access Services through the Computer Management console: click **Start**, right-click **Computer**, select **Manage**, then locate and expand the Services and Applications node in the console tree. (You will learn about the Computer Management console and snap-ins a little later in this lesson.)

## Startup Types

There are four startup types for Windows services:

| | |
|---|---|
| **Automatic** | The service will start automatically when the operating system starts. |
| **Automatic (Delayed Start)** | The service will start automatically after all the services configured for Automatic start. That is, the startup of the service is delayed briefly to allow other services to start first. |
| **Manual** | The service will not start automatically, but it may be started when needed by a user or by an application that requires it. |
| **Disabled** | The service will not start automatically and cannot be started manually. You can disable a service to optimize operating system performance, but you must be certain that the service is not needed; otherwise you inadvertently cause system failures or other problems. |

Even if they start successfully, services may fail from time to time. If a service fails, Windows supports various recovery actions. These include restarting the service, running a program, restarting the computer, or doing nothing.

## Service Accounts

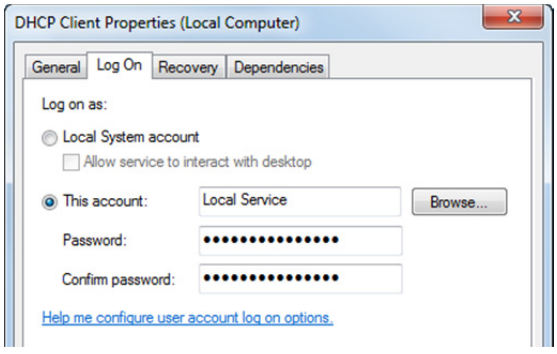
When you log into a computer as an end user, you are entering your security credentials so that Windows will understand which resources you are allowed to access and what type of access to grant you. However, automatic services (those with a startup type of Automatic) will start immediately when a computer is powered on, so they need their own logon ID to present as security credentials to Windows.

For example, a service may attempt to perform any of the following operations:

- Read and write registry entries
- Access remote servers
- Access internal system hardware
- Read and write files from or to the file system

You must, therefore, ensure that a service uses an account that has sufficient privileges to perform the operations that it is designed to perform.

To enter or change the logon ID, right-click the service and click **Properties**, then select the **Log On** tab:




You can specify either a user account (e.g. your own ID) or one of the Windows special accounts as the logon ID. If you want to use on of the Windows internal accounts, you can choose any of the following:

- The Local System account – represented as NT AUTHORITY\LocalSystem. This account has full authority and access to everything on the local computer, including accessing the network. You should avoid using this account because it has unlimited access privileges on the computer.
- The Network Service account – represented as NT AUTHORITY\NetworkService. This is a limited service account with network access rights. It is similar to a standard user account's access privileges on the local computer.
- The Local Service account – represented as NT AUTHORITY\LocalService. This is a limited service account similar to a standard user account on the local computer, but with no network access rights.

All of these special accounts are configured with a null password.

In an enterprise environment, you should avoid using any of these Windows service accounts. The security policies in some enterprises may go further and actually prohibit their use because a misbehaving service or a security attack on the service can cause damage to the computer or other systems on the network. Instead, you should request that a dedicated user account be created in the enterprise Active Directory with sufficient access privileges to run these services. For your own home computer, you should use the Local Service account.

## Service Dependencies and Managing Services

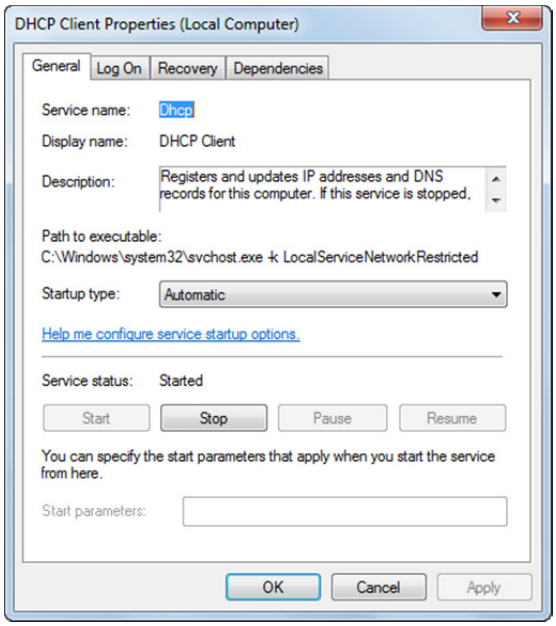
Some services depend on other services. If a dependency service is not running, a dependent service may fail to start or fail to function properly once it has started.

You must consider service dependencies when you begin to manage services on a system.

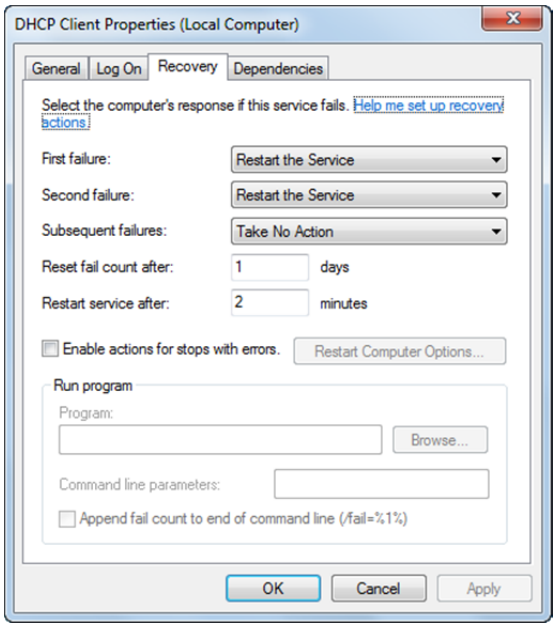
**MMM**
Working with Services

You use the Service snap-in to manage services. You can double-click any service in the window to access its configuration properties. The Properties dialog box includes four tabs.

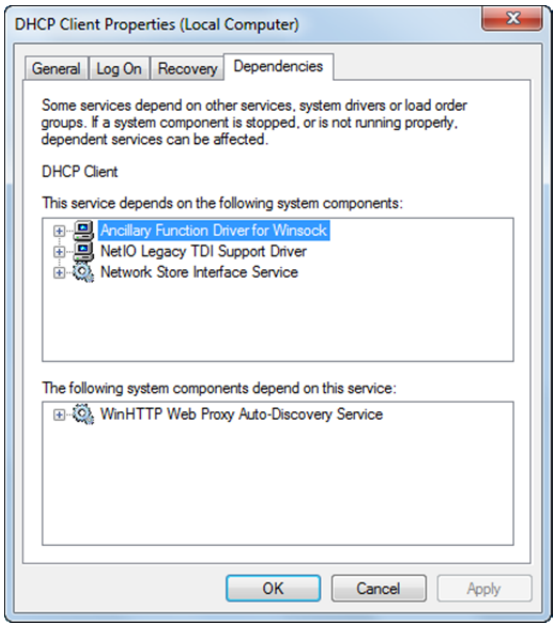
You use the General tab to specify a startup type, and to start, stop, pause, or resume the service.




You use the Recovery tab to specify how the computer responds when the service fails. Notice that you can specify what action to take after the first, second and subsequent failures.




You use the Dependencies tab to view service dependencies. Notice that the dialog box shows both which components the selected service depends on, and any components that depend upon it.




# Managing Remote Systems and Users

Objective 1.5

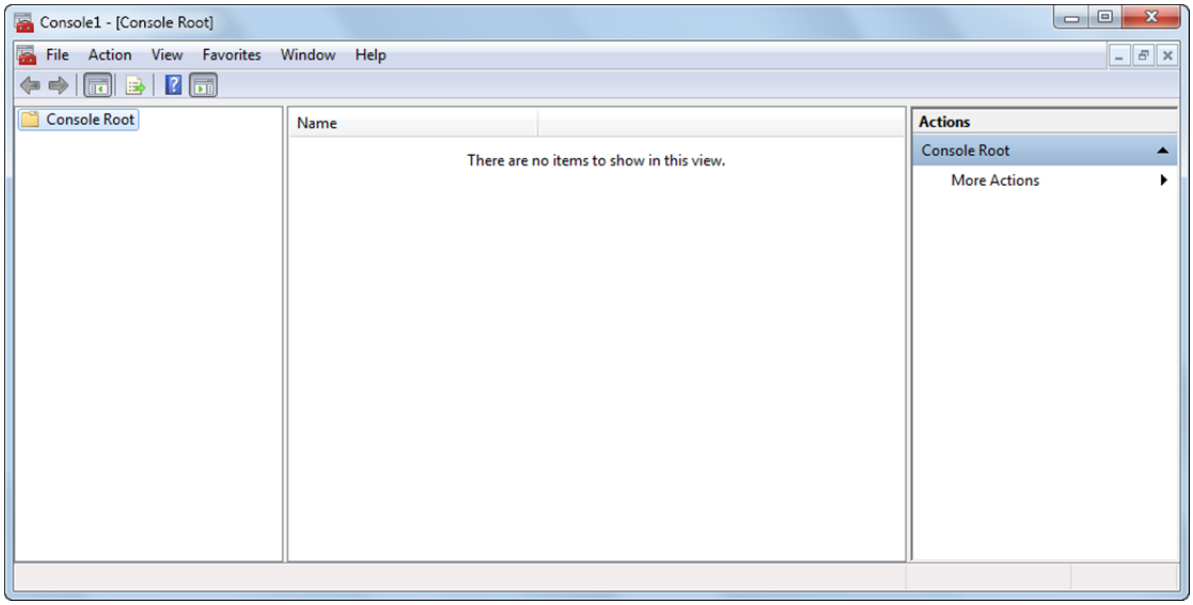
Most end users spend time only at a local machine. That is, they are physically seated in front of it; they type on its keyboard and view output on its monitor. Network and systems administrators on the other hand often have to manipulate several machines (both desktop systems and servers) within their enterprise, and it is not always convenient to be seated in front of each machine that requires attention.

For this reason, remote management tools and technologies were created.

Windows 7 (and Windows Server 2008 R2) management tools and interfaces provide access to the same configuration settings that can be configured through the Control Panel or other local interfaces. However, many of the management tools provide the ability to control and configure remote systems as well as local ones.

# Microsoft Management Console (MMC)

The Microsoft Management Console (MMC) is an interface that hosts and displays various administrative tools, called snap-ins. A snap-in is a module that you load into an MMC interface in order to provide functionality. For example, snap-ins are used for managing the hardware, software and network components of Windows. The MMC by itself, with no snap-ins loaded, is simply a shell.




The file type for a snap-in is Microsoft Common Console Document, and the file name extension is .msc. Most snap-ins are located in the C:\Windows\System32 or C:\Windows\Winsxs directory. Several of the tools in the Administrative Tools folder in the Control Panel, such as Computer Management, Event Viewer, and Task Scheduler, are MMC snap-ins.

The Computer Management snap-in is actually a collection of MMC snap-ins, including the Device Manager, Disk Defragmenter, Internet Information Services (if installed), Disk Management, Event Viewer, Local Users and Groups (except in the home editions of Windows), Shared Folders, and other tools.

The Computer Management snap-in is key for configuring and controlling remote machines, and it is used to configure Remote Desktop Connections, which you will read about later in this lesson.

Other commonly-used MMC snap-ins include:

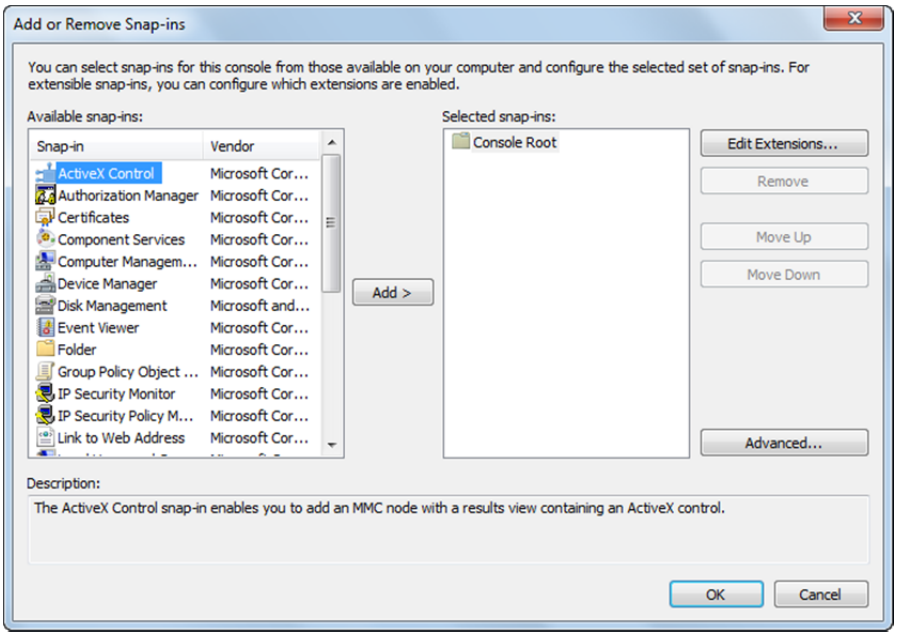
- Microsoft Exchange Server
- Active Directory Users and Computers, Domains and Trusts, and Sites and Services
- Group Policy Management, including the Local Security Policy snap-in included on all Windows 2000 and later systems. (This snap-in is disabled in the home editions of Windows.)
- Services snap-in, for managing Windows services
- Performance snap-in, for monitoring system performance and metrics
- Event Viewer, for monitoring system and application events

Adding snap-ins to the console is as easy as selecting them from a list box. The combination of a snap-in and the MMC is also referred to as a console.

## Exercise 3-5: Creating a Custom MMC Console

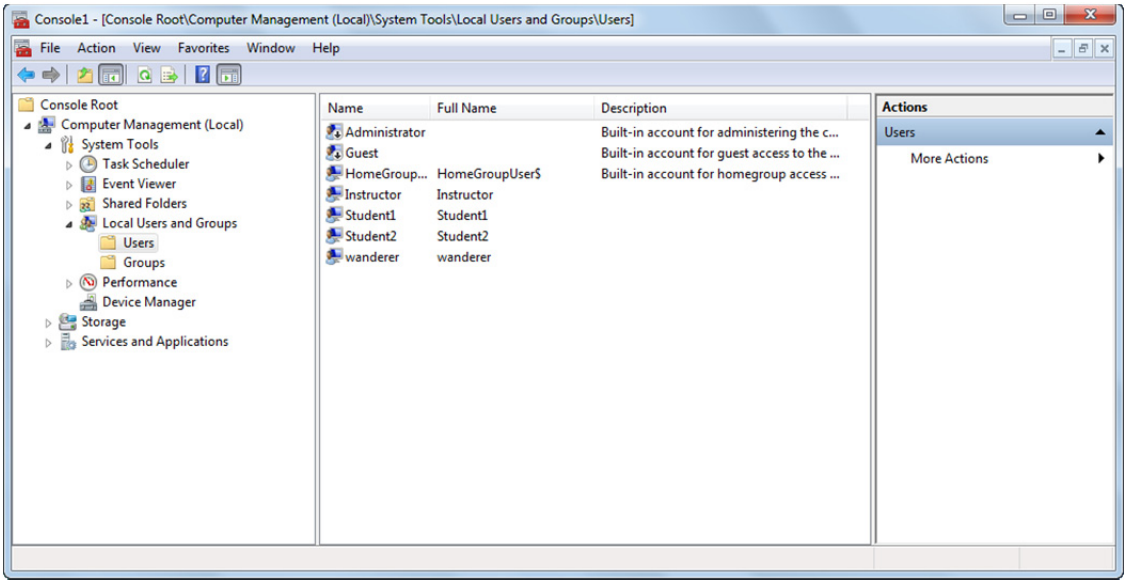

In this exercise, you will create and save a custom MMC console and explore a few of the available options.

1. Click the **Start** button, then in the Search box type: `mmc.exe` and press ENTER to open an empty Microsoft Management Console. If prompted by the UAC, click **Yes** to proceed.
2. In the menu bar at the top of the MMC, click **File**, **Add/Remove Snap-in** to open the Add or Remove Snap-ins dialog box.



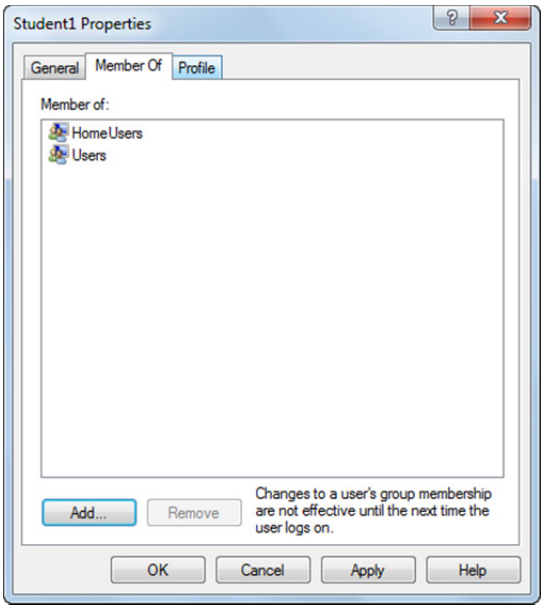

3. In the Available snap-ins list box, click **Computer Management**, then click the **Add** button. When prompted to select the computer you want the snap-in to manage, ensure that **Local computer** is selected, then click **Finish**.
4. Click **OK** to close the Add or Remove Snap-ins dialog box. The Computer Management snap-in is now added to the MMC.

   The left pane of the console is called the console tree. The tree always begins with the console root and currently includes one node – the Computer Management node.
5. In the console tree, expand the **Computer Management** node, expand the **System Tools** node, expand the **Local Users and Groups** node, then click **Users**. (Note that the Users and Groups node is unavailable in Windows 7 Home Premium edition. It displays only in Windows 7 Professional, Ultimate/Enterprise.) The middle pane is the display area. It displays information related to the node selected in the console tree. It currently displays the user accounts on the local system. The right pane is the Actions panel. Various available actions display here depending on what is selected in the left or middle pane.




6. In the Actions panel, click **More Actions** to display a menu of possible actions. Notice that you can add a new user.
7. Press Esc to close the menu.

8. In the display pane, click one of the user accounts. Notice that the user name and additional actions now display in the Actions panel.
9. Display the possible actions for the selected user account. Notice that you can set a password, delete or rename the account, or view all of account's properties. In the **More Actions** menu, select **Properties** to open the <user> Properties dialog box and click the various tabs to view the properties for the current account.




10. Click **Cancel** to close the Properties dialog box.

You can add as many snap-ins as you like to a MMC.

11. In the File menu, click **File**, **Add/Remove Snap-in** to open the Add or Remove Snap-ins dialog box.
12. In the Available snap-ins list box, click **Services**, then click the **Add** button. When prompted to select the computer you want the snap-in to manage, ensure that **Local computer** is selected, click **Finish**, then click **OK** to close the Add or Remove Snap-ins dialog box. (You will work with local services shortly.)
13. In the console tree, collapse the Computer Management node.
14. In the menu, select **File**, **Save As** to open the Save As dialog box.
15. Navigate to the Desktop, type: `MyConsole` as the File name, then click the **Save** button to save the custom MMC to the Desktop.
16. Close the MyConsole console, click **Yes** to save the current settings. Note that the file is saved as *MyConsole.msc*.

In this exercise, you created a custom MMC.

## Group Policy

Objective 3.1

You were briefly introduced to Group Policy earlier in this lesson. Group Policy is a feature in Windows that allows system administrators to manage users' access to programs, Windows features, and even hardware.

Group Policy is used to manage systems in Active Directory domains. In Windows Server 2008 R2, administrators use a MMC snap-in called Group Policy Management Console (GPMC) to create and modify policies.

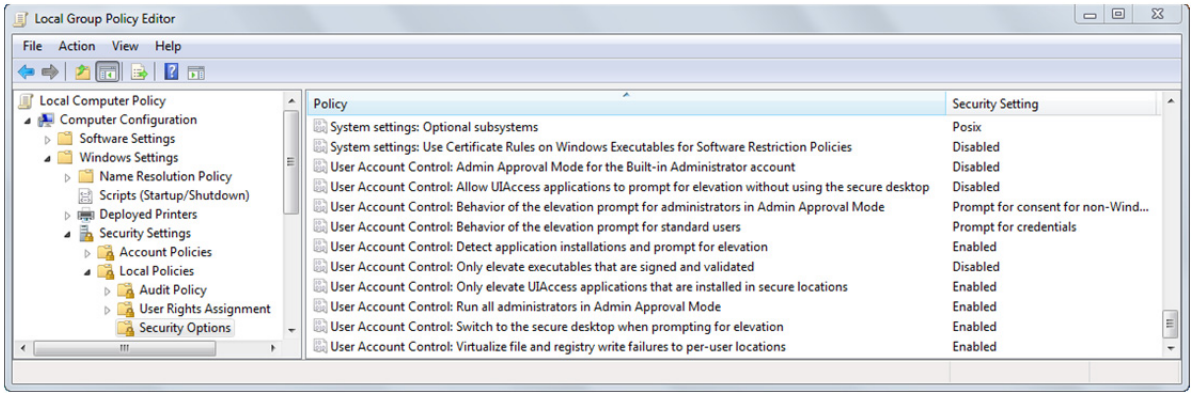
Microsoft has also released a tool called Advanced Group Policy Management (AGPM), which is available to any organization that has licensed the MS Desktop Optimization Pack (MDOP). This advanced tool allows administrators to institute a check in/check out process for modification of Group Policy Objects. That is, several administrators can work on various GPOs, and the tool will track changes to Group Policy Objects. To use this tool, you must license all Windows Active Directory clients for MDOP.

## Local Group Policy Editor

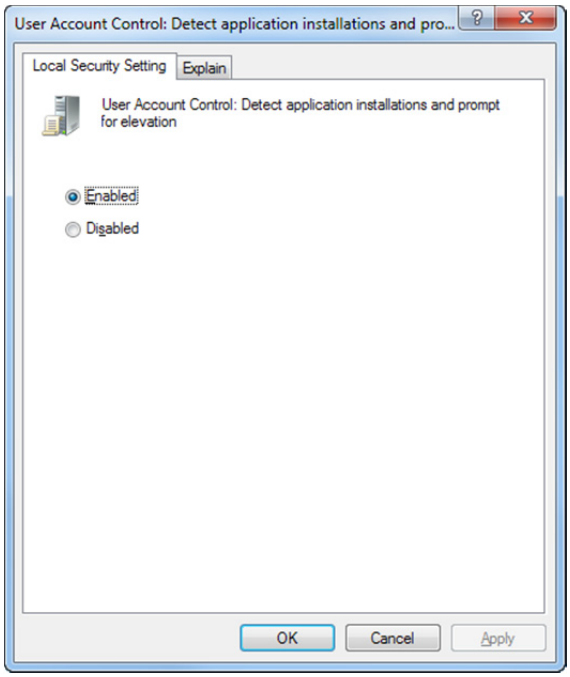
Local group policy is a more basic version of the Group Policy used by Active Directory. In Windows 7 and Vista, Local Group Policy can enforce a Group Policy Object (GPO) for a computer or for individual users.

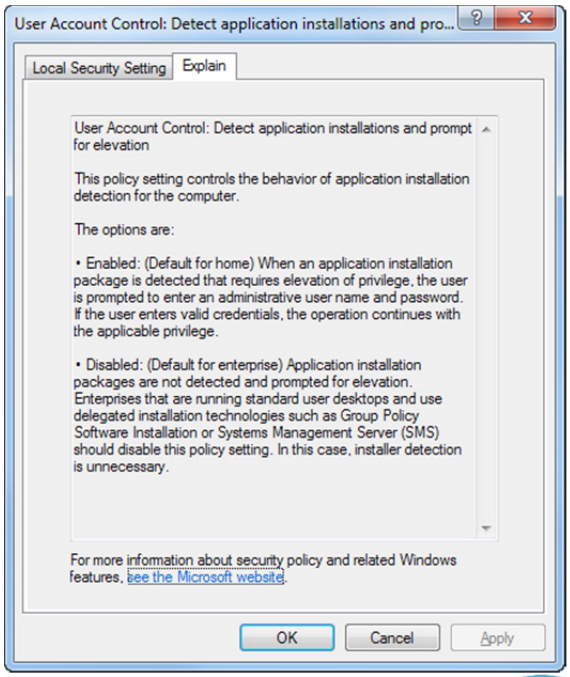
The Local Group Policy editor is a MMC snap-in you can use to edit local GPOs. It is available in Windows Sever 2008 R2 and Windows 7 Professional, Ultimate and Enterprise. To open the Local Group Policy editor, click **Start**, type: `gpedit.msc` in the Search box, then press ENTER.

The following figure shows UAC configuration settings in the Local Group Policy editor. The settings are located in the Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options window.




To modify a policy's setting, double-click it to open its properties.



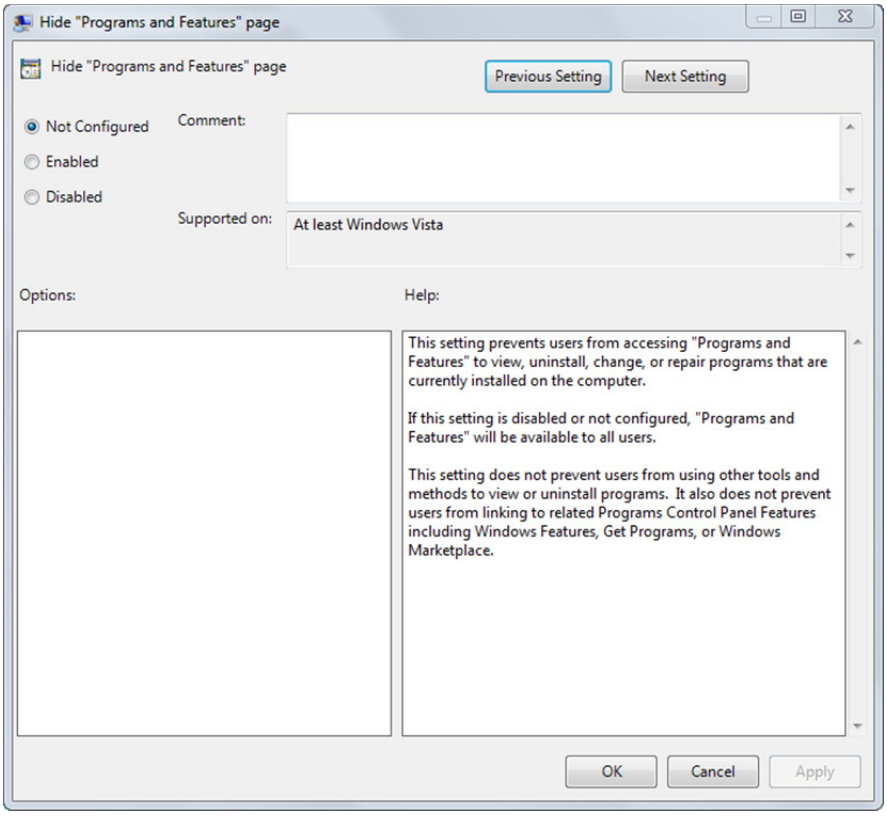




## Exercise 3-6: Exploring the Local Group Policy Editor


In this exercise, you will use the Local Group Policy editor. Note that you must be logged in as an administrator.

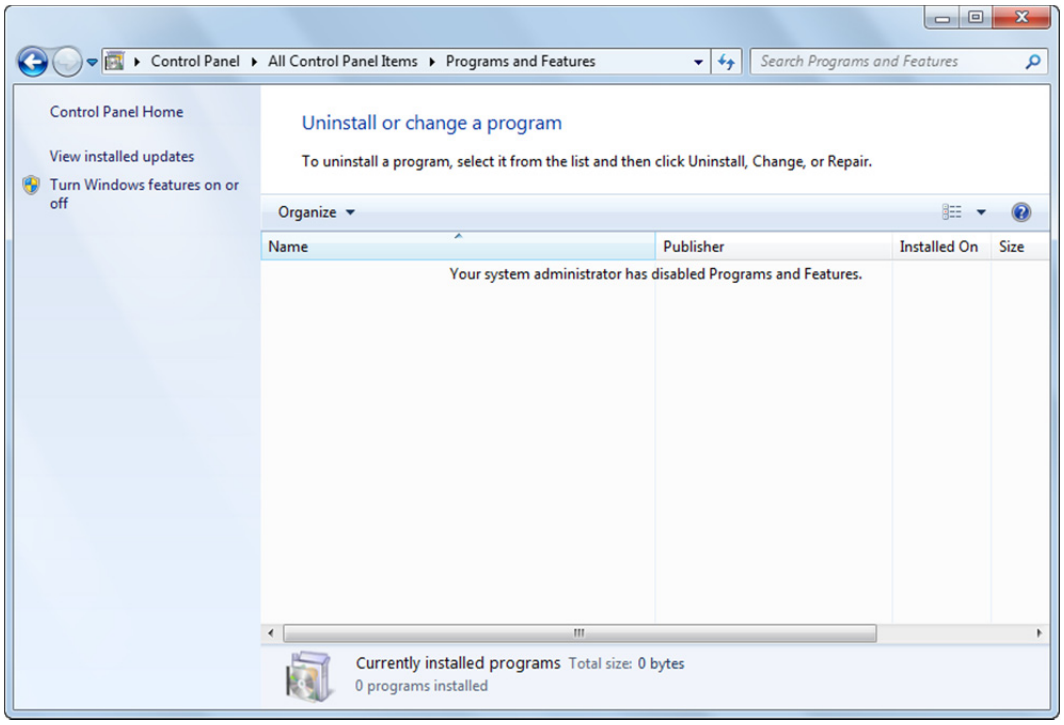
1. Click the **Start** button, then in the Search box type: `gpedit.msc` and press ENTER.
2. Expand **User Configuration**, expand **Administrative Templates**, expand **Control Panel**, then click **Programs**.
3. Ensure that the Extended tab is selected at the bottom of the window, then click **Hide "Programs and Features" page** to display a description of the setting. What can you tell about this particular policy?

4. In the display pane, click the Edit **policy setting** link to edit the setting.




5. Select **Enabled**, click **Apply**, then click **OK**.

6. Minimize the Local Group Policy editor window, open the Control Panel, then open the Programs and Features page. You are not able to use the features of this Control Panel page.



7. Close the Control Panel, then restore the Local Group Policy editor window.
8. Change the policy setting back to **Not Configured**, click **Apply**, then click **OK**.
9. Open the Control Panel once more and open the Programs and Features page. This time, you are able to use the features on the page.
10. Close the Control Panel.
11. Close the Local Group Policy editor.

In this exercise, you edited a Group Policy setting and observed the results.

## Windows PowerShell

**MMM**
Taking PowerShell for a test drive

Another management interface available in Windows 7 is Windows PowerShell 2.0. PowerShell is a task-based command-line shell and a scripting language rolled into one. PowerShell is designed especially for system administration. PowerShell is similar in appearance to a command prompt window, but is much more powerful because:

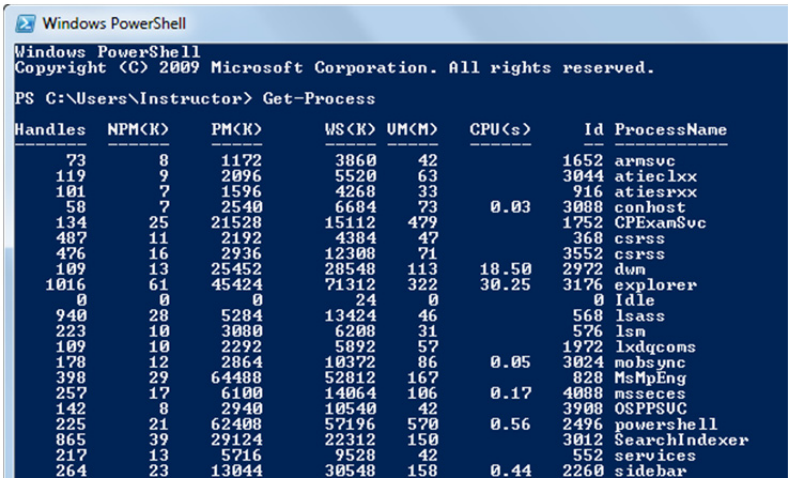
- you can use it to automate tasks, and
- you can use it to run those automated tasks on both local and remote systems.

Consider for a moment the steps required to set the new company intranet home page as the home page on your browser. There aren't many steps involved – you would open the browser, type the URL of the intranet home page into the Address bar, then you would open the Internet Options dialog box and click the Use Current button on the General tab to set the page as the browser home page. You could then click OK and close the browser. It would probably take less than a minute.

Now, how long would it take to set the home page on 10 systems in your department? How long to reconfigure the browsers on 100 systems in your building? How long would it take to reconfigure the browsers on 15,000 systems across the enterprise? Here is where the power of scripting becomes apparent: by using Windows PowerShell, you can create a simple script that sets the new home page and then send the script to (and run it on) all the systems that require it – all in a matter of minutes.

PowerShell is an interactive shell that looks similar to the command prompt window (in fact, you can execute the same commands you can enter at the command prompt); you can enter commands and retrieve information.

Unique to PowerShell are cmdlets (pronounced "command-lets"); these are the native commands in PowerShell, and they follow a <verb><noun> naming pattern. For example, the cmdlet *Get-Process* (shown in the following figure) retrieves a list of all processes running on the machine. The cmdlet *Get-Service* retrieves a list of all services running on the machine. The cmdlet *Get-Help* displays help about PowerShell cmdlets and concepts.




You use cmdlets to carry out specific system functions, such as managing services, editing the registry or reviewing event logs.

PowerShell also includes a task-based scripting language, which can perform complex operations. You can issue cmdlets in PowerShell or develop your own scripts to be run on a particular machine or remote machines. You can also use PowerShell to automate many of the same tasks you perform using the Group Policy Management Console. To help you perform these tasks, Group Policy in Windows Server 2008 R2 provides more than 25 cmdlets.

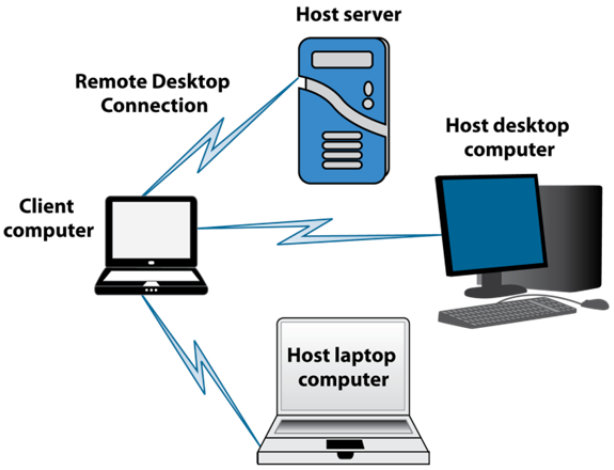
To open a Windows PowerShell session, click the **Start** button, click **All Programs**, double-click **Accessories**, double-click **Windows PowerShell**, then click **Windows PowerShell**.

# Remote Desktop Connection

Objective
**1.4**
**2.4**

Remote Desktop Connection (RDC) is a feature that allows you to use a computer (the *client*) to access and control a remote computer (the host).

RDC is built into both Windows servers and clients and is intended to enable remote management. For example, via RDC, you can use your computer at home to connect to your computer at your work location and access all the application software and data on the work computer.




RDC was formerly known as Microsoft Terminal Services Client (MSTSC). Later, it was referred to as RDP (Remote Desktop Protocol) because this protocol describes the structure and content of the data exchanged between the computers.

RDC was developed by Microsoft to enable one or more "dumb terminals" to be connected to a server computer running the Windows Server operating system. A dumb terminal consists of a keyboard, mouse, monitor, and a basic system unit with a network connection. With this type of arrangement, multiple users can share a Windows computing environment running on a server and the operating system responds to each user as if he or she were the only user on the system.

Obviously, the user sitting at the local machine must be able to see the Desktop of the remote machine, and must be able to send keyboard input and mouse actions from the local machine to the remote system. RDC provides the screens to the client computer for applications running on the host computer, and it sends mouse actions and keyboard input from the client to the host. While RDC was originally developed for dumb terminals, the client system can be any computer capable of running Windows, such as a desktop or laptop computer.

Once a client is connected to a host computer, the client computer can use the host computer to open its own RDC session with yet another remote host, establishing a type of daisy-chain of remote control. This ability allows users to overcome connection limitations created by the manner in which the computers are physically connected.

All Windows systems have RDC capability built in, and a computer running any Windows 7 edition can function as an RDC client. However, for a computer to be an RDC host, it must be running Professional, Ultimate or Enterprise edition. Additionally, if an RDC host computer is running an end user operating system (e.g., Windows 7, Vista, or XP Professional), the host will only allow one user – remote or local – to log in at any one time. For example, you cannot use RDC to connect to a Windows 7 computer as a host if someone else is using it; you must wait for that person to log out. However, a computer running Windows Server software has the Terminal Services software built into it, which allows multiple client computers to connect to it using RDC. The Windows Server software includes a license for two RDC connections at the same time. Licenses for additional simultaneous connections must be purchased and loaded into a licensing server.

The Remote Desktop Connection window has several tabs for the various options:

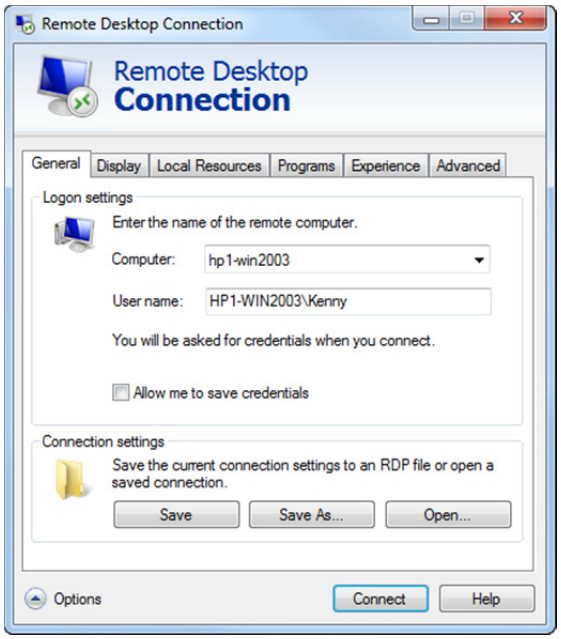
The **General** tab identifies:

**Computer**
Name of the host computer that you want to connect to.

**User name**
User ID to use for logging into the host computer.

**Allow me to save credentials**
An option to save the host computer name, your logon ID, and your password to save the effort of entering this data again in the future.

**Connection settings**
An option to save the RDC settings to this host computer as a file. You can then double-click on this file (e.g., on the Windows Desktop) to simplify the task of connecting to this host computer.

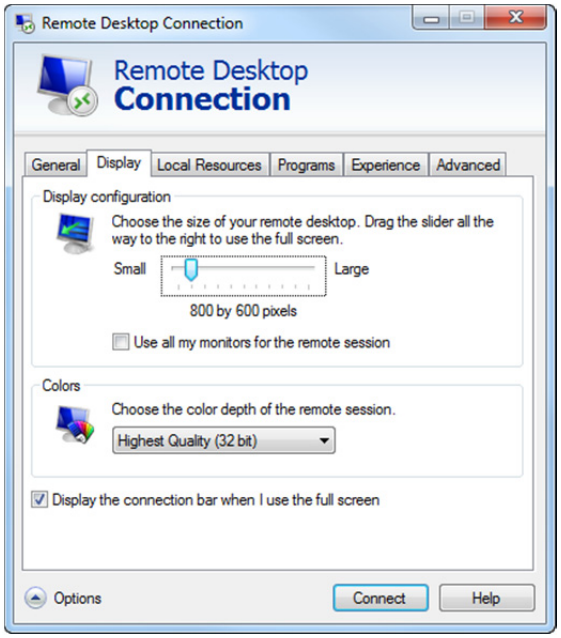



The **Display** tab identifies:

**Display configuration**
Selects the size of the screen on which to display the host computer's monitor output. This is similar to connecting a different-sized monitor to your computer; the hardware will automatically adjust the display area to the amount of space available. Moving the slider bar to the far right will cause the host computer display to take the full screen of your local display monitor.

**Colors**
Selects the color range to display the host computer's monitor output. A lower-quality setting reduces the amount of data sent through the network, which is beneficial for low-bandwidth lines such dial-up modem connections.

**Display the connection bar when I use the full screen**
If selected, the connection bar below is displayed at the top when in full screen mode. The host computer name displayed here will remind you that you are interacting with that computer and not your local client computer.





RDC (version 6.0 and higher) can support high-resolution monitors up to 4096 x 2048 pixels by using the ***/w***(idth) and ***/h***(eight) modifiers when launching the RDC software. It is also capable of spanning across multiple monitors, by using the ***/span*** modifier when launching the RDC software.

The **Local Resources** tab enables or disables features:

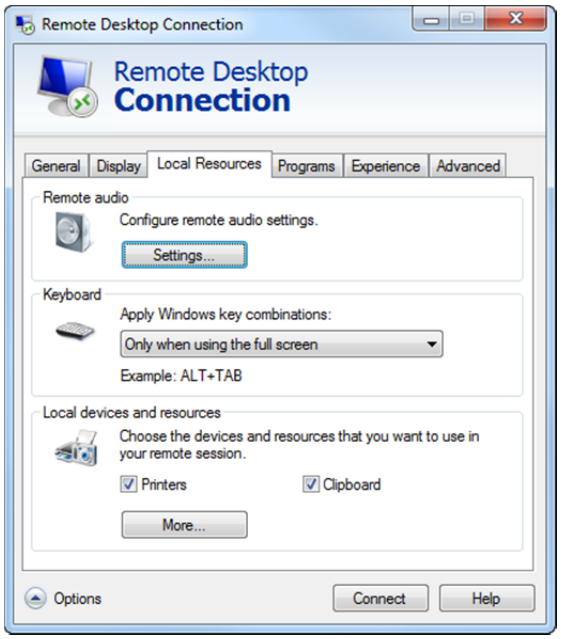
**Remote audio**
Enables or disables audio output from the host computer to play on your client computer, and audio recording to be sent to the host computer.

**Keyboard**
Enables or disables the Windows key combinations on your local keyboard to be sent to the host computer.

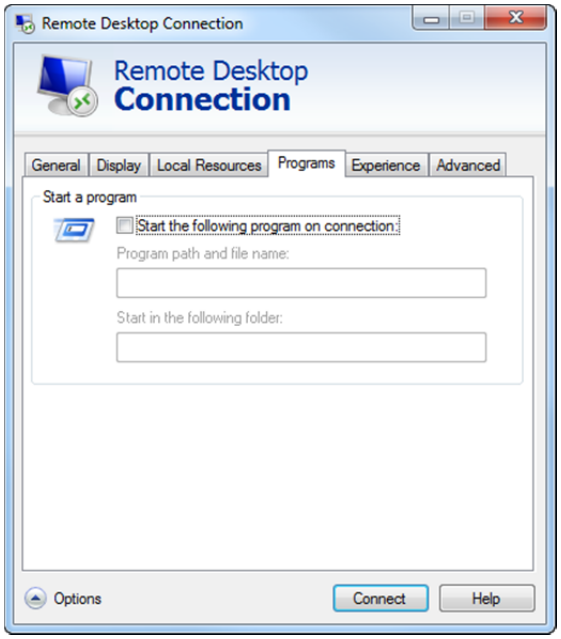
**Local devices and resources**
Makes locally-connected devices such as printers, Windows Clipboard, local hard drives, and USB devices available for use by the host computer in a process called redirection.

USB devices that are redirected will not be available for use by the local computer until the Remote Desktop session has ended. Before redirecting USB devices, you should be sure they are not actively in use on the local computer, or data loss may occur.

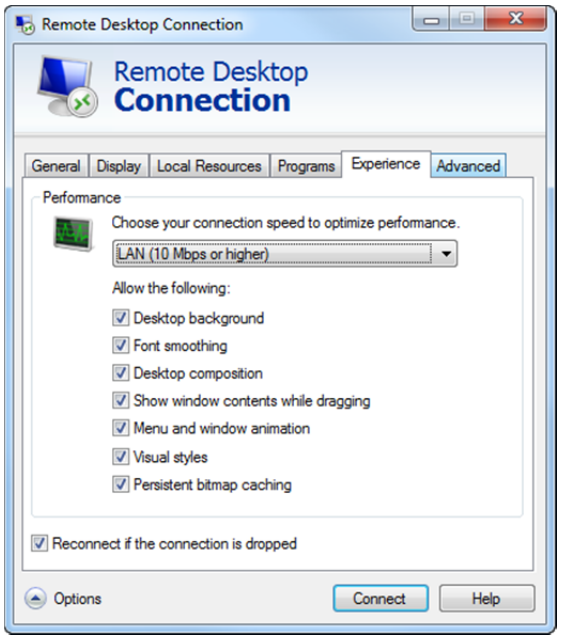
Additionally, each device you redirect will increase the amount of data exchanged with the host computer and therefore increase the load on the network.




The **Programs** tab allows you to select specific application software to run immediately after connecting to the host computer. Note that if this option is specified, the host computer will run only this software; when you exit from the software, the connection will also terminate.



The **Experience** tab enables or disables features that appear on the display monitor to recreate the Windows 7 Desktop user experience. These features also consume a large amount of network bandwidth that can be accommodated in an internal network (e.g., ***LAN 10 Mbps or higher*** setting). If you have a lower-speed network connection, these features are turned off to improve response time.



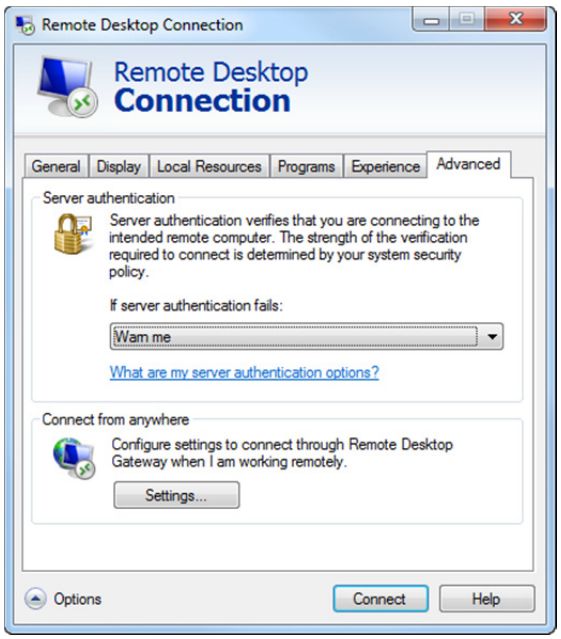

The **Advanced** tab has the following settings:

**Server authentication**

This is used to verify that you are connecting to the correct host computer.

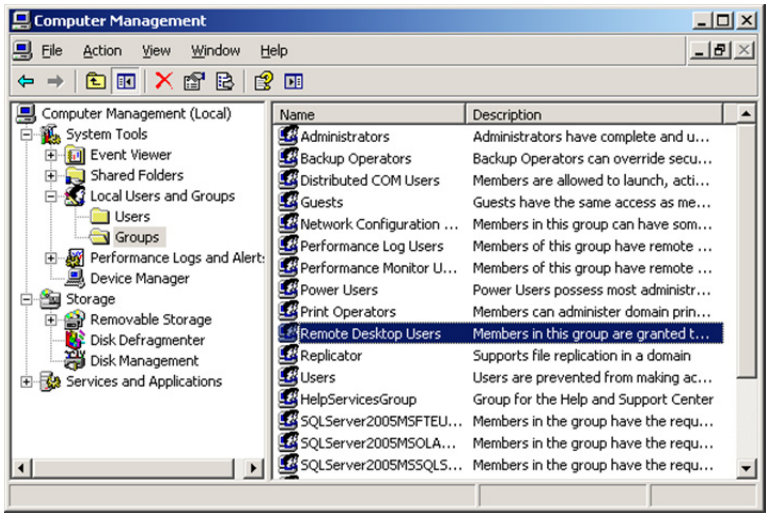
**Connect from anywhere**

This is used to connect to the Remote Desktop Gateway server in a Remote Desktop Services (RDS) installation. This topic will be discussed in more detail shortly.

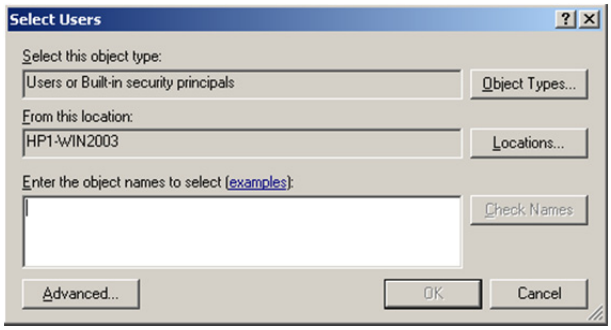



To enable other users to use RDC to connect to a Windows Server 2003 computer, you must enable the logon IDs of all users who are permitted to connect to the computer. This is a security feature to prevent a server from being accessible to everyone by default; you must explicitly add the authorized users:

1. Click the **Start** button, then click **All Programs**, **Administrative Tools**, **Computer Management**.
2. In the Computer Management window, expand the **Local Users and Groups** tree and click **Groups**.

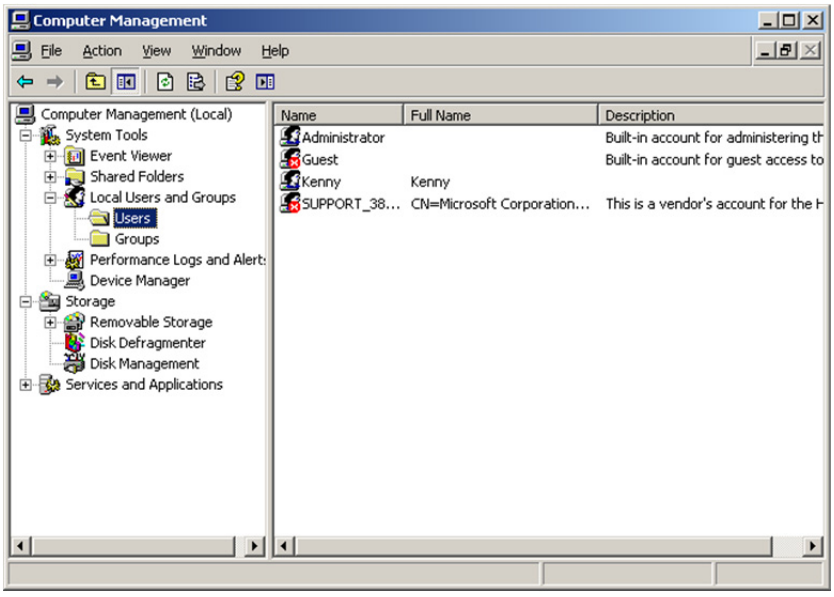



3. In the right pane, double-click **Remote Desktop Users** to view the properties.
4. Click **Add** in the Remote Desktop Users Properties window.
5. Enter the logon IDs of the user(s) and click **OK**.



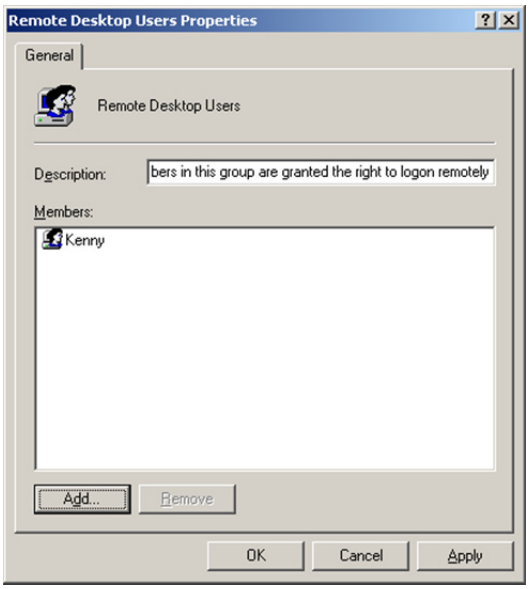

On a Windows Server 2008 (or 2008 R2) server, any user identified as an administrator is automatically allowed to RDC to the server.

In a home or small business network, the user IDs must be added to the list of local users before they can be added as remote desktop users.



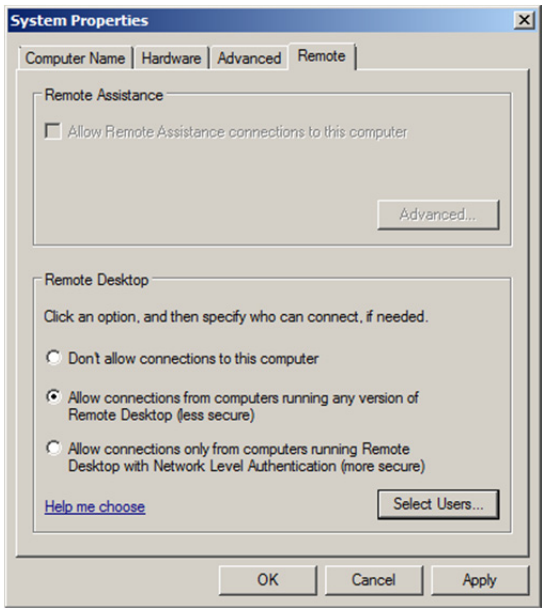
In enterprise networks, user logon IDs are a little more complex because most enterprise networks use Active Directory domains, and most, if not all, computers will be part of the enterprise domain. In this case, the **From this location** field must contain the domain name. Alternatively, the user ID must be prefaced by the domain name (e.g., `domainname\userID`). In an enterprise, you should use domain IDs as much as possible to take advantage of the improved security and easier administration provided by Active Directory.

The completed Remote Desktop Users Properties window now lists all authorized users.



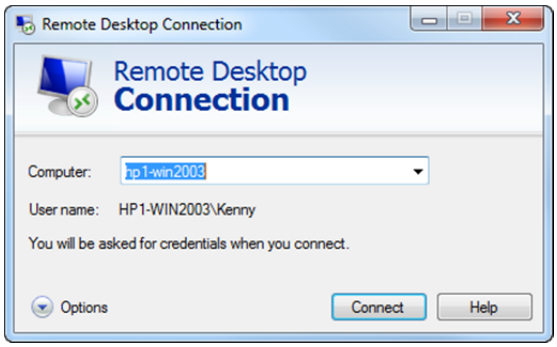

On a Windows 7 or Windows Server 2008 computer, RDC is turned off by default. You must both enable it and add the users to the RDC list:

6. Click the **Start** button, right-click **Computer**, and click **Properties**.
7. Click **Remote settings** in the left pane to display the System Properties dialog box.
8. Enter the administrator password in the User Account Control box if necessary.
9. Click the **Remote** tab.



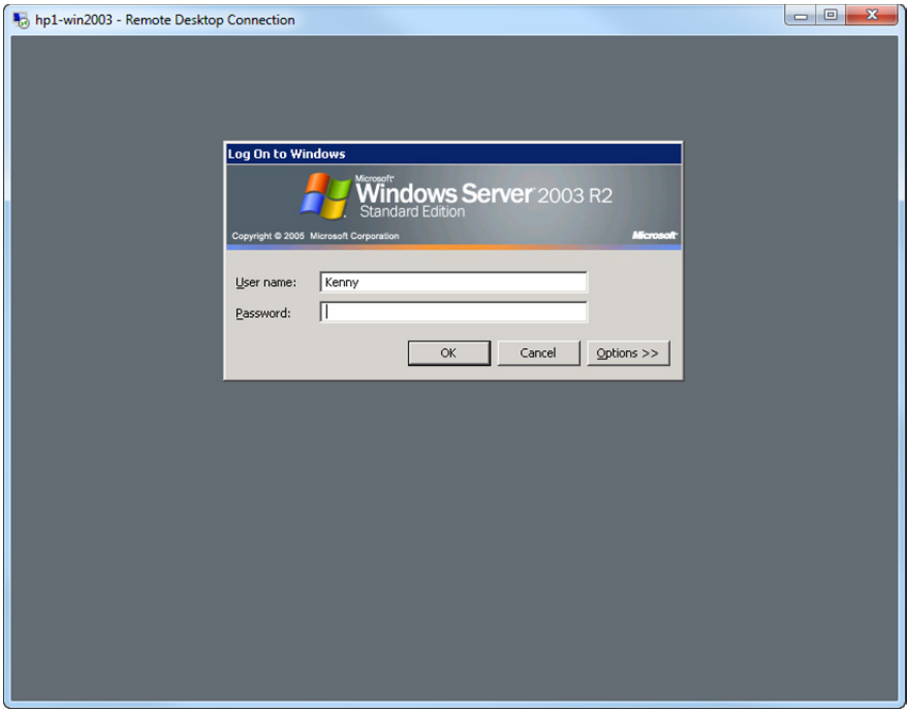

Once the servers or host computers are set up, you can initiate the RDC session using these steps:

10. On your computer, click **Start**, **All Programs**, **Accessories**, **Remote Desktop Connection**.
11. At the Remote Desktop Connection dialog box, enter the name of the host computer to which you want to connect.
12. If necessary, click **Options** and change any of the connection options.




13. Click **Connect**.

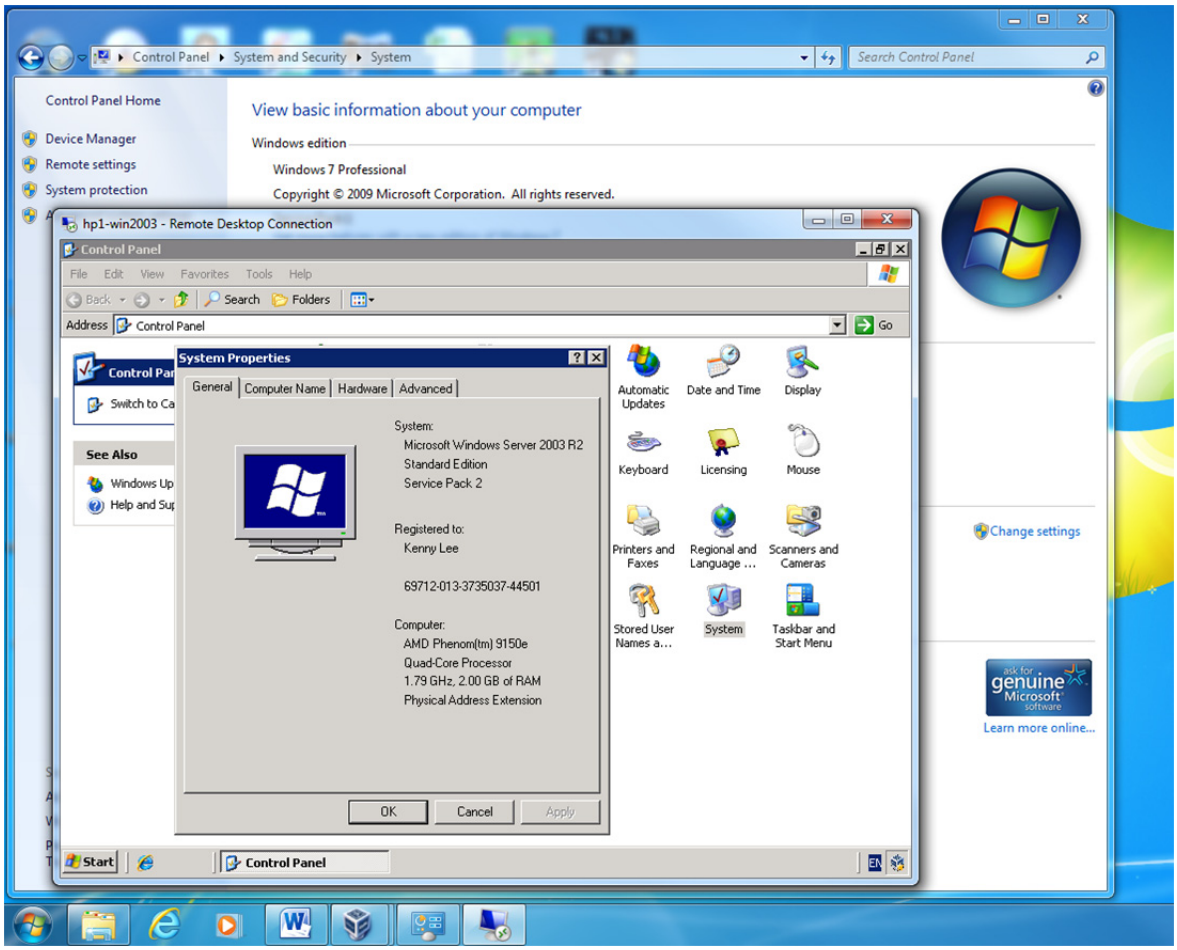
If the host computer is running and responding to RDC requests, the Log On to Windows dialog box is displayed on your monitor. If you do not enter anything into this window for one minute, it will *time out* and close automatically.



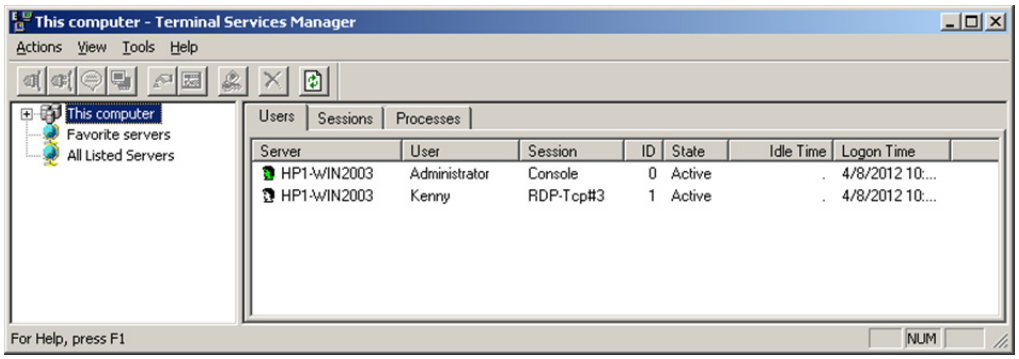

Note that RDC requires that the host computer's IP address be reachable from your IP address. For example, if your computer and the host are in the same enterprise-wide network, then you will be able to establish the connection. If you are at home or working in a hotel room, then you will not be able to access the host computer at your workplace because the latter will be behind the corporate firewall; you will need to establish a VPN (Virtual Private Network) connection first. Alternatively, you can configure your RDC to connect using the Remote Desktop Gateway server (described in more detail below). Similarly, if you are using your work computer, you will not be able to use RDC to connect to your computer at home because your home computer will likely be connected to a router with a built-in firewall.

If the host computer is joined to a domain (authenticated using Active Directory) in an enterprise network, the Log On to Windows dialog box will also display the **Log on to** field for the domain name:


After you have successfully logged in, the Desktop of the host computer will display (if **Start the following program on connection** was not specified as an option). For example, the following screen capture shows a Windows Server 2003 RDC session displayed on a Windows 7 Desktop.




On the server side, you can identify any users who are currently connected. Click **Start**, **All Programs**, **Administrative Tools**, **Terminal Services Manager**. The Console session is the keyboard, mouse, and monitor devices that are connected directly to the server hardware. These devices are usually accessible only to technicians because servers are generally locked in a small room at the back of an office, retail store, or warehouse, or are located in an air-conditioned data center with many other servers stacked on racks.



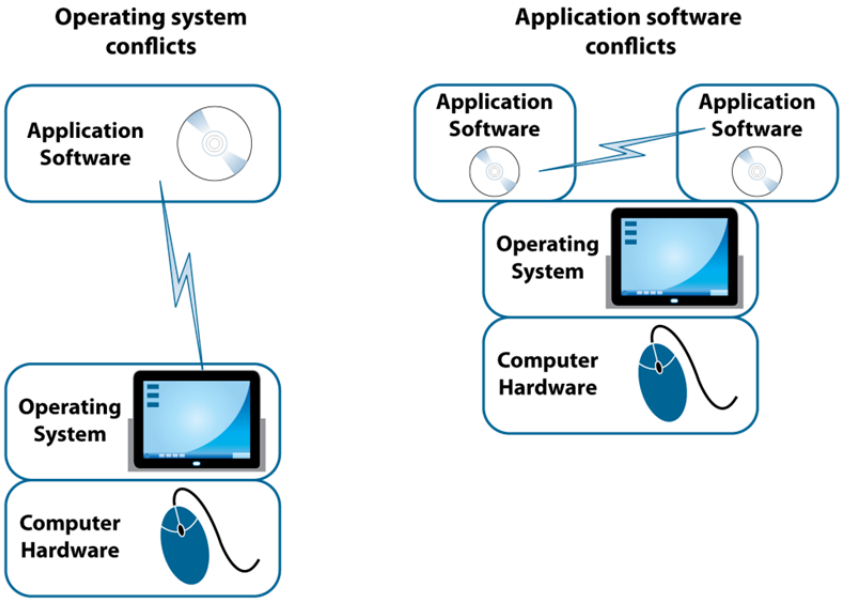

In summary, remote desktop connection is a useful tool that allows you to operate a computer located elsewhere in the network. All hardware, application software, and data that you access and control during the remote session reside on the host computer. The client computer simply acts as an extension of the monitor, keyboard, and mouse to the host computer. Because RDC does not require much processing power to run, your client computer does not need to be a very powerful computer.

# Application Virtualization

Objective 3.5

Microsoft Application Virtualization (App-V) runs designated application software in a virtual environment. Like MED-V (which you learned about in Lesson 1), App-V is designed to allow enterprises to deploy applications by minimizing conflicts with the operating system environment.

MED-V is designed to eliminate conflicts between application software and the operating system (and the hardware underneath) by creating a virtual machine environment in which the application is designed to work.




However, conflicts can also occur between different applications running on the same system.

In the enterprise environment, application software can be highly specialized and require specific versions of third-party drivers and utility software (e.g., IIS, java, .NET, or SQL Server). If a server hosts two (or more) applications that depend on these external utilities, a conflict can occur if for example one application requires that the external utilities to be upgraded to a newer version while other applications are not compatible with the newer versions. To prevent these conflicts, enterprises usually install only one application on each server. This general rule is one of the main reasons for the rapid proliferation of servers in data centers.

# App-V

App-V is a Microsoft product designed to prevent conflicts between applications by sequencing (or publishing) an application to a client computer. To the user, the sequenced application appears to be installed on the local machine. In the background, however, the application is *streamed* from a central server to run in a virtualized *sandbox* on the user's computer. (Streaming means that the application software is retrieved to your computer only when it is needed.)

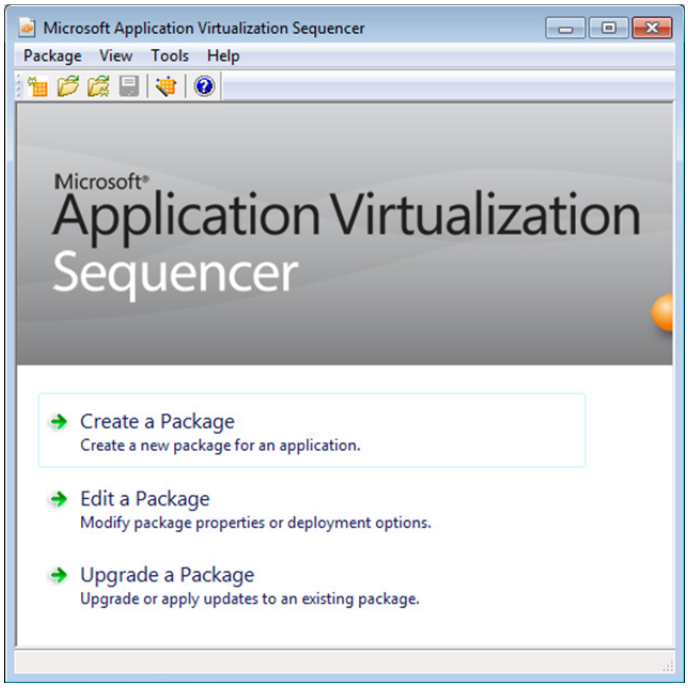
A virtualized sandbox is a self-enclosed environment, kept separate from the contents on the rest of the computer. For example, most applications that are locally installed on a computer put entries into the registry. App-V applications do not affect the computer's registry because they run inside a sandbox.

Unlike a virtual machine such as Microsoft Virtual PC, the App-V runtime environment does not have an operating system installed and will run only one application inside it. However, your computer can access and run many App-V applications at the same time. This design feature allows a user to run Word 2003, Word 2007, and Word 2010 all at the same time, as an example.

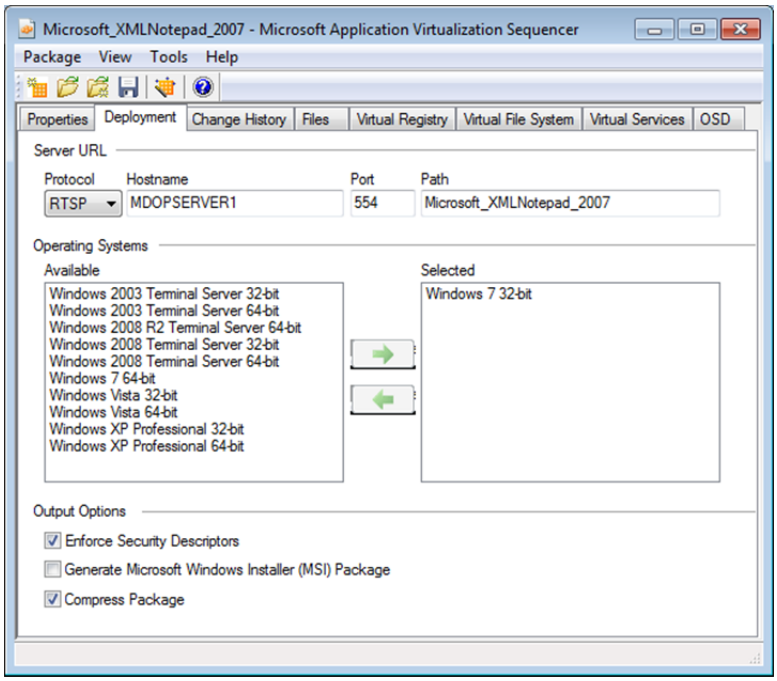
Normally, users will uninstall the older version of MS Office products when upgrading to a new version in order to prevent conflicts between the versions. With App-V, users can run any combination of applications that are individually compatible with the locally-installed operating system, but may conflict with each other.

Once installed, the App-V application will appear in the Start, All Programs menu like any other locally installed application. When the program is started, it will also behave like a locally installed application – able to open and save data files on local or network hard drives. The application can also be configured to run in "standalone" mode; that is, it can be used even when there is no network connection to the App-V central servers.

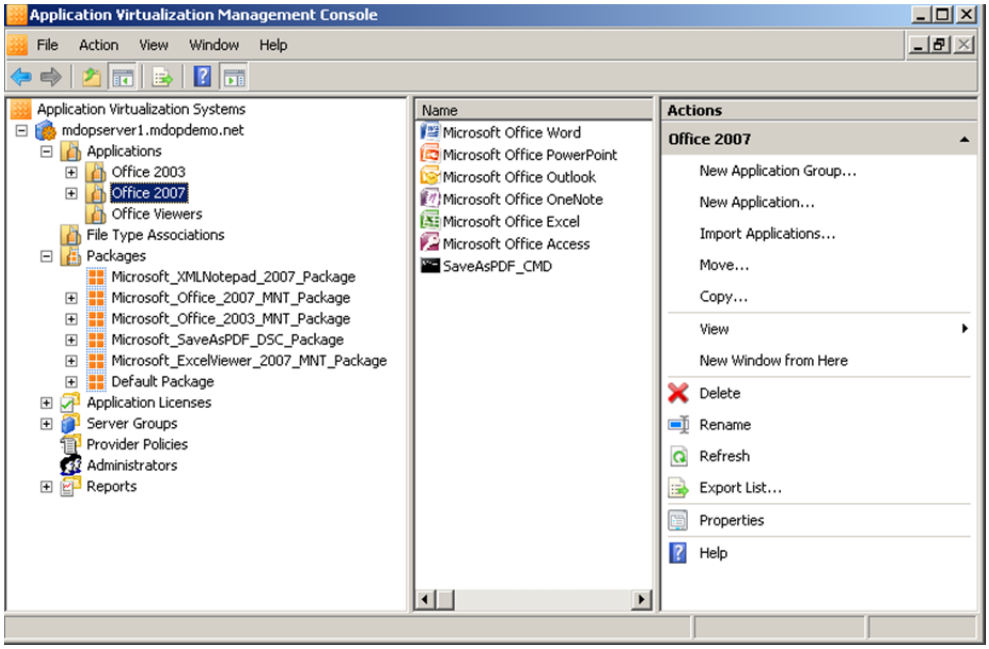
To publish an application for App-V, system administrators must prepare it using the Application Virtualization Sequencer. This sequencing process is required to convert the application software into the special format used by App-V.



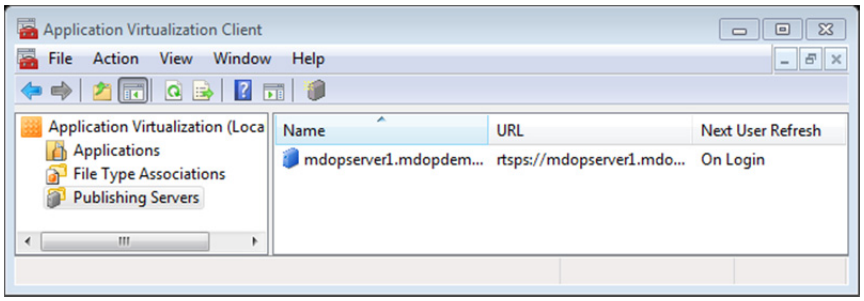

Once the package is created, the system administrator will configure the deployment settings to run in the operating systems that are used by the various users:



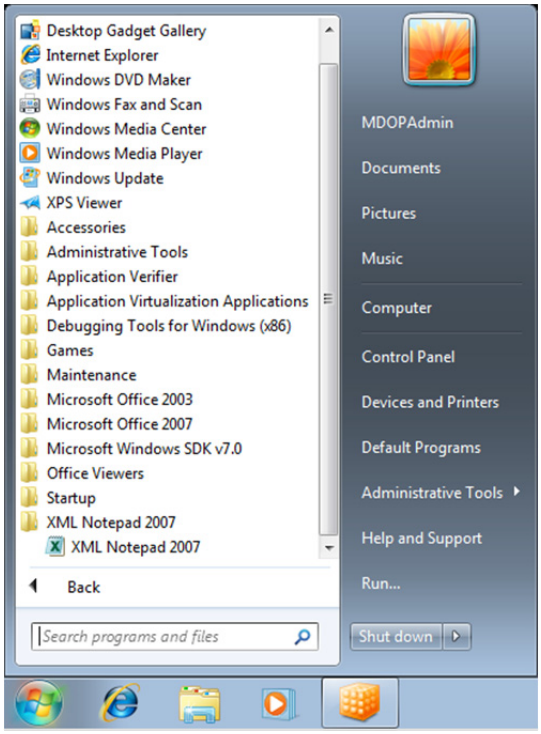

After the virtualized package is created, it can be deployed using a centralized streaming server (using either the App-V Management Console or the System Center Configuration Manager) or manually installed on client computers. The system administrators must also use Active Directory to assign the application to users. To deactivate the App-V application, they simply remove that assignment.



On the client computers, the App-V Client connects to the App-V server to obtain a list of all available applications accessible by the current user.




The following screen capture shows the application XML Notepad 2007 available in the Start, All Programs menu. Note that there is no obvious indication that it is an App-V application:




One of the Microsoft websites offers a hands-on demonstration (called virtual labs) of setting up, managing, and using App-V. Go to http://technet.microsoft.com/en-us/virtuallabs/ and select the Windows 7 link.

In summary, App-V applications are installed on a centralized server, and then streamed down to run on client computers on demand. When running on the client computer, each of these applications runs in its own sandbox in order to avoid conflicts with other App-V applications or with locally installed applications running at the same time.

Even though these applications run in a sandbox, they access the hardware on the local computer, have access to all data on local and network hard drives, and appear in the same Start, All Programs menu as locally installed applications.

## Remote Desktop Services (RDS)

Objective 2.4

While the traditional method of provisioning user computers is to install application software directly onto the user systems, this method is very labor-intensive and consumes a great deal of time.

Remote Desktop Services (RDS) is a Windows Server technology that enables users to access Windows-based programs that are installed on Remote Desktop Session Host servers. By using RDS, an administrator can install applications on a central bank (also called a *farm*) of servers, and all users simply access that central bank in order to use the application. Users can connect to a Remote Desktop Session Host server from within an enterprise network, or over the Internet.

Configuring and maintaining applications on a central server (or bank of servers) can be substantially easier than installing and upgrading software on end user systems scattered throughout an enterprise. When an application update becomes available, the appropriate server is updated and all clients automatically use the updated application.

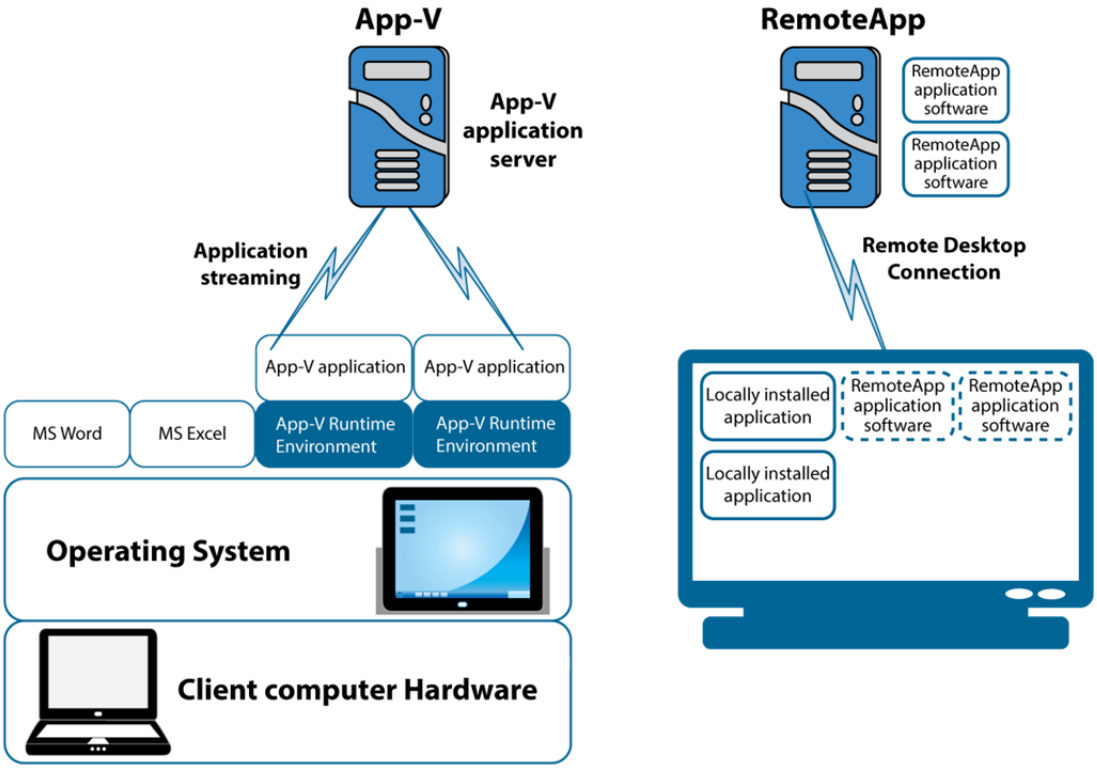
Provisioning Remote Desktop Services requires a bank of very powerful servers that can handle hundreds of simultaneous users. RDS was designed to address three main areas: load balancing, security, and licensing.

Remote Desktop Services in Windows Server 2008 R2 includes RemoteApp and Remote Desktop Connection, which enables you to make applications or virtual desktops that are accessed remotely through Remote Desktop Services appear as if they are running on the end user's local computer. These programs are referred to as RemoteApp programs.

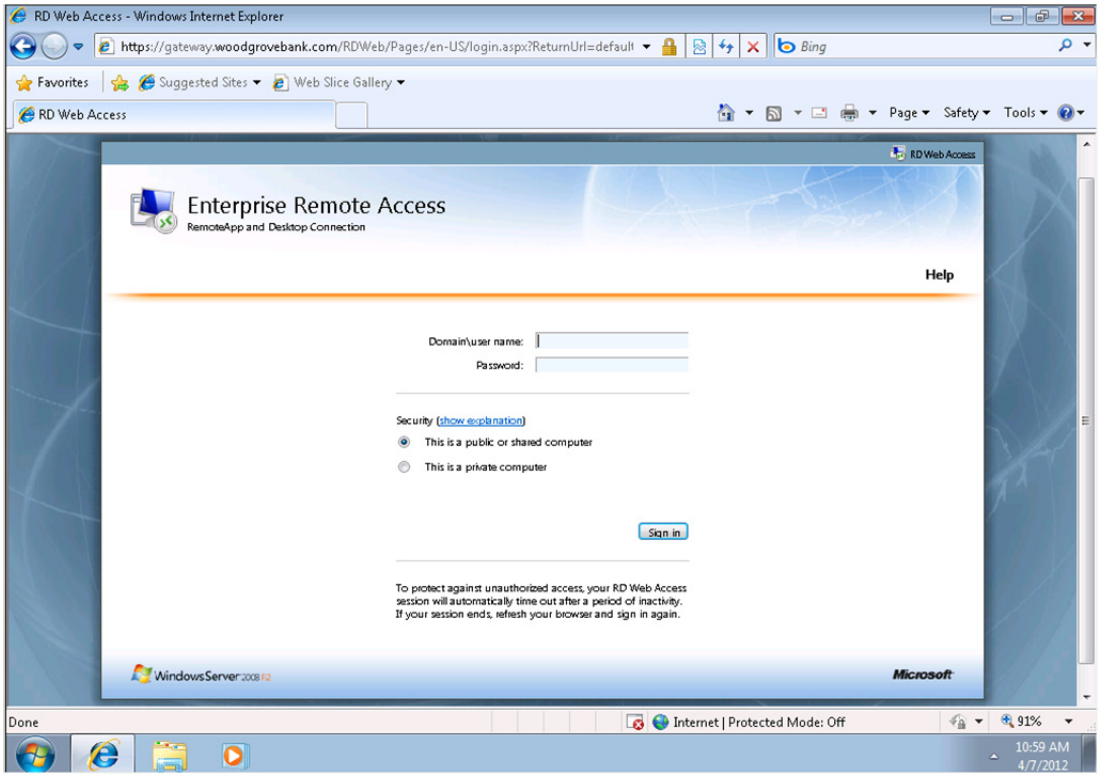
Instead of being presented to the user in the desktop of the RD Session Host server, the RemoteApp program is integrated with the client's desktop. The RemoteApp program runs in its own resizable window, can be dragged between multiple monitors, and has its own entry in the taskbar.

## RemoteApp

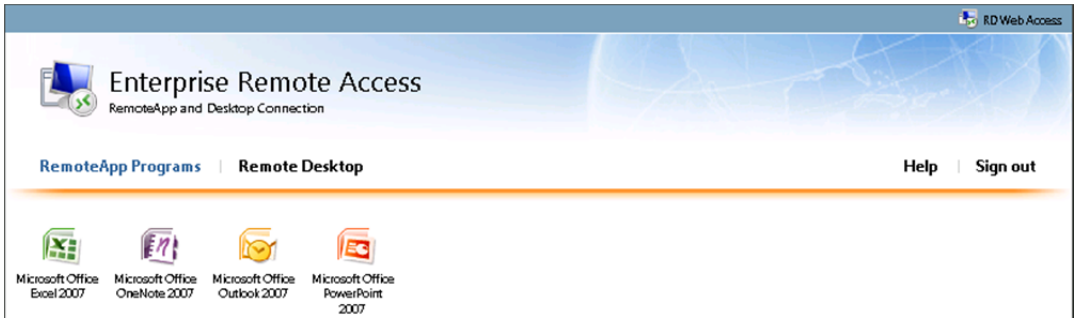
Another way of publishing a virtualized application to end users is to use the remote desktop protocol (RDP). As is the case with App-V, a client computer can access and run many different RemoteApp applications. Unlike App-V, RemoteApp applications actually run on a server within the Remote Desktop Services infrastructure. On the client computer, the user sees the results of the application that is actually running on that remote server.



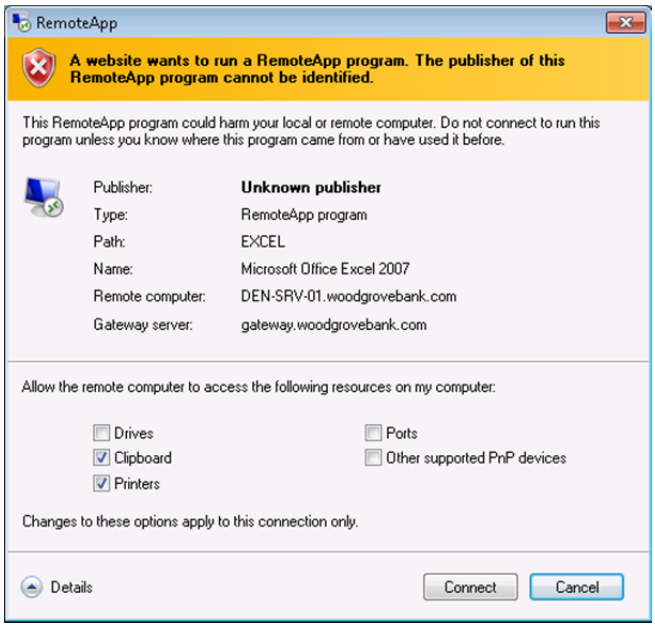
To use a RemoteApp application, you must first sign in to the Enterprise Remote Access using Internet Explorer.



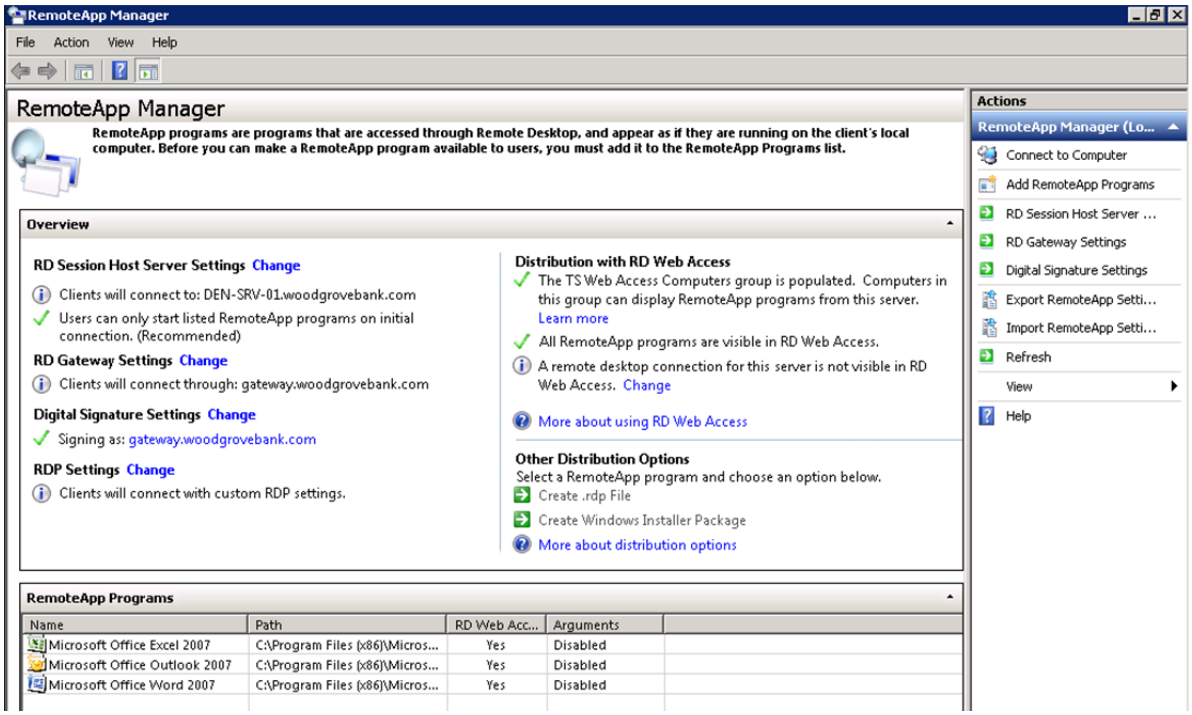

Once you are validated as a user, the web page displays the RemoteApp applications that you are permitted to access:



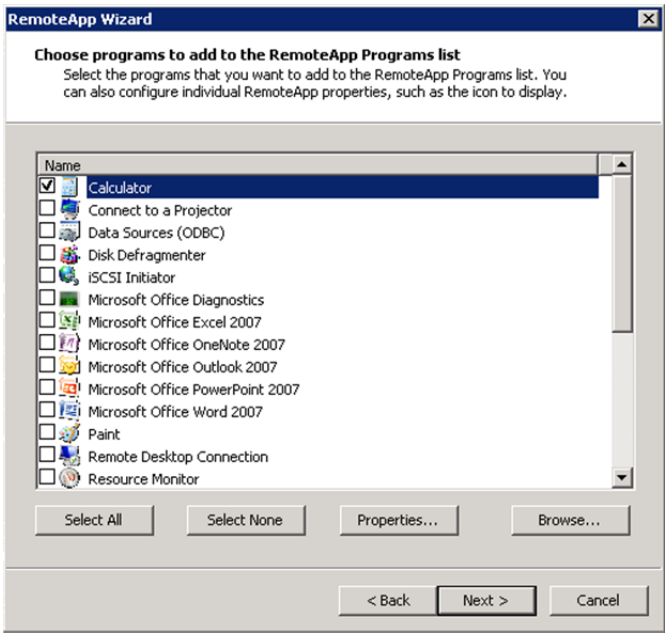

When you run a RemoteApp application for the first time on a computer, a warning message may display asking you to verify that you are connecting to the correct servers.



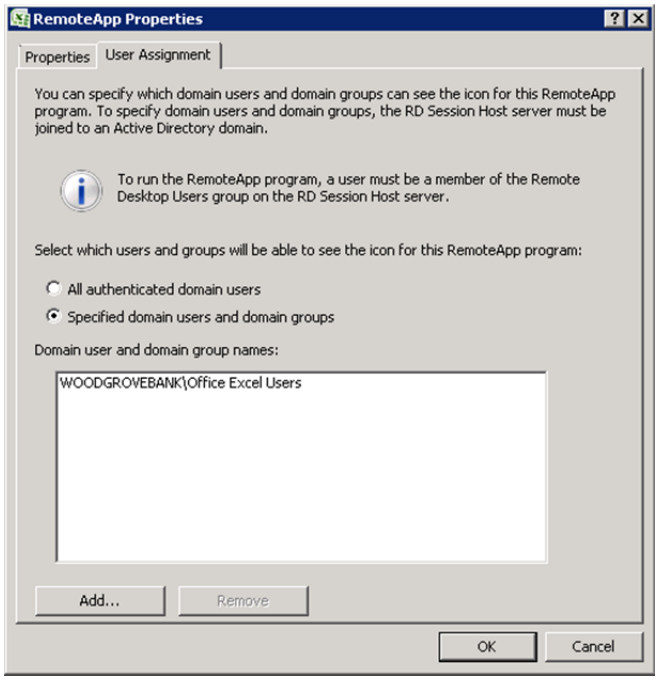

The system administrators use the RemoteApp Manager to set up the applications that will be available for publishing. The main screen lists the applications that have been installed in the Remote Desktop Session Host servers:



Adding more applications to the list is as simple as selecting the checkbox in a wizard:



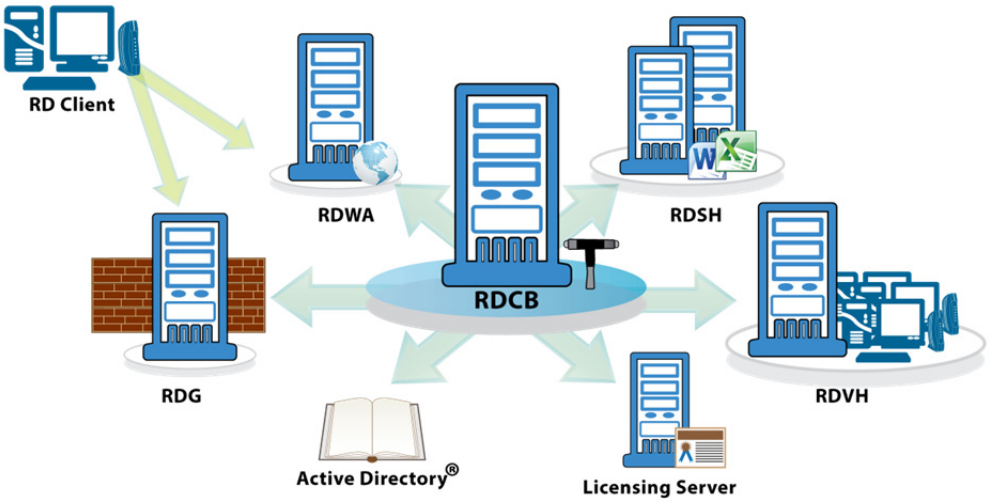

From this list, the individual applications are assigned to individual or groups of users. This list controls which RemoteApp applications are displayed for each user.




In summary, RemoteApp applications are installed on centralized servers and users use a specialized version of Remote Desktop Connection to see which ones are available for them to access. When a user selects an application, it runs on a centralized server using the hardware and network connections on that server. The user's computer is used only to run Internet Explorer to control the application.

# RDS Infrastructure

A key feature of RDS is the ability to manage and deliver virtualized applications across an enterprise. To accomplish this, it employs an infrastructure that can provide load balancing, security, and licensing.




The entry point for a user (**RD Client**) into the RDS infrastructure is a simple URL entered into a web browser such as Internet Explorer in the following format: *https://domainname/rdweb*. For example, a user could enter the following URL*: https://finance.companyname.com/rdweb*.

This URL is sent to the Remote Desktop Web Access (RDWA) server, which returns a list of the RemoteApp programs that this user is authorized to use. Initially, the user is prompted to enter his credentials (i.e., user name and password), which are validated against the Active Directory database. Entries in Active Directory are used to assemble the access control list for this user (that is, to determine which objects the user may access). The access control list is then used as a filter on the list of all available RemoteApp programs so that only programs to which the user has access will appear. For example, an accounts payable clerk in the Finance division may see only five programs listed in a menu, when there are perhaps hundreds of programs that exist for all Finance users.

If the user is outside the corporate firewall (e.g. employee working from home, contract worker, or vendor) the connection request is directed from the Internet to the Remote Desktop Gateway (RDG). Here, the request is screened to verify that it came from an authorized user.

The role of the Remote Desktop Connection Broker (RDCB) is similar to that of a telephone exchange; when a remote user initially makes a connection request, the RDCB will direct the request to the correct server. Once the access request is validated, the RDCB is responsible for maintaining the integrity of the connection. While this may appear to be a simple task, keep in mind that there could be thousands of connections at any given time.

The Remote Desktop Session Host (RDSH) is where the application software is actually installed. It is responsible for loading the software into RAM, executing the instructions, and generating the output to send back to the user. The same application may be installed on multiple physical servers to serve multiple users at the same time. A *load balancer* will typically be used to even out the workload across these servers and ensure that response time is minimized for everyone. When load balancing technology is used, users will not notice if a physical server crashes or becomes unavailable for any reason because the workload will simply be redistributed among the remaining servers.

The Remote Desktop Virtualization Host (RDVH) is the server that runs the Hypervisor-V software that creates the virtual machines (VMs). When serving a VM-based request, an associated RDVH will automatically start an intended VM, if the VM is not already running, and a user will always be prompted to enter credentials when accessing a virtual desktop. However, a RDVH does not directly accept connection requests and it uses a designated RDSH as a “redirector” for serving VM-based requests. The pairing of a RDVH and its redirector is defined in Remote Desktop Connection Broker (RDCB) when adding a RDVH as a resource.

# Virtual Desktop Infrastructure

Objective
2.4
3.5

Let us turn attention once again to the world of the physical. Any PC you can touch and see contains components to store data and software to perform computations internally. Because it is a physical machine, it can exist in only one place at a time. This fact makes it inconvenient to work from more than one location.

For example, if you want to cram more work into your day by continuing to work at home using data from your office desktop computer, you would need to copy the data to a USB drive and carry that drive back and forth. Or perhaps, you could use a laptop, and carry that back and forth.

The inconvenience of using physical machines can translate to lost time when certain situations arise. For example, what happens if your laptop is stolen? What happens when a component in a physical machine fails, or an application must be updated? In each case, the user has to wait – wait to get a replacement, wait for a repair, or wait for an upgrade.

Now consider what it could be like to use a virtual computer. Suppose everyone in your enterprise had their physical computer replaced by a virtual one. Just as servers can be virtualized, end user systems can be virtualized as well.

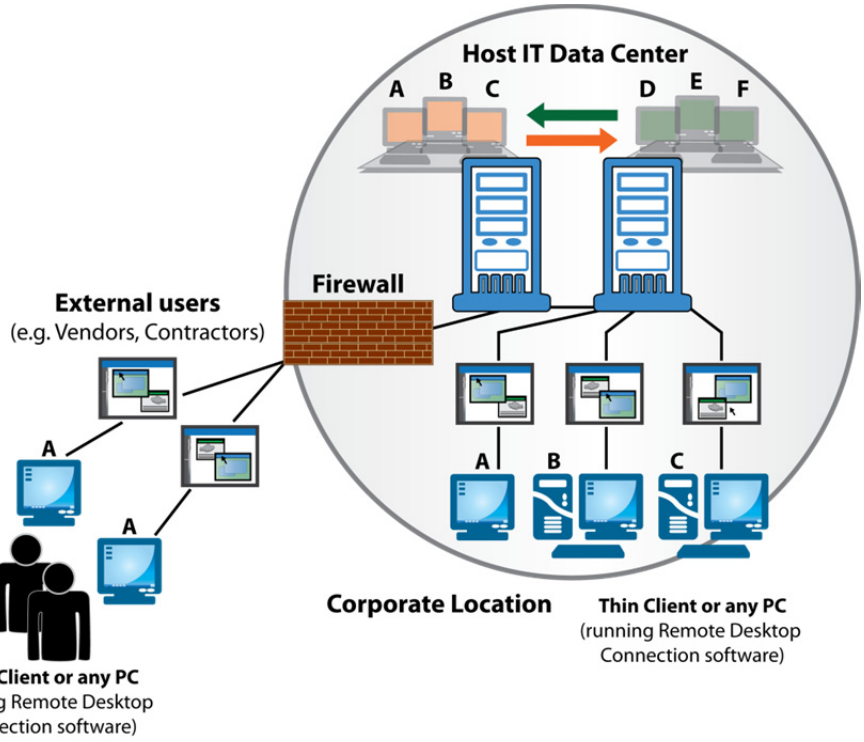
## What is VDI?

Virtual Desktop Infrastructure (VDI) has been described in some literature as "delivering desktops from the data center." VDI occurs when enterprise desktop computers are virtualized (moved onto servers in the data center), and then presented to users over the network.

All the benefits of virtualization apply to virtualized desktops. For example, an enterprise with 2,000 desktop and other types of computers can reduce them to 200 servers (assuming each server hosts 10 VMs). This reduction quickly results in significant savings in electricity and air conditioning costs. Although office computers do not require special cooling requirements, collectively they generate a large amount of heat that places an extra burden on a building's HVAC (Heating, Ventilation, And Cooling) system.

The provisioning process is also drastically simplified: a request to add a new VM or to upgrade a VM can be done in minutes with virtual equipment. This can provide a strategic advantage that allows a business to rapidly ramp up or down in a department or business line. For example, a call center can be expanded in several weeks instead of several months because less equipment must be physically purchased, installed, and tested.

Every user in the enterprise can have his or her own VM, and each VM is unaware that it is only one of many other VMs hosted together on the same physical server.



Once VDI is implemented, end user systems are typically replaced with thin-client machines, resulting in significant cost savings.

The big difference with virtualized desktops, compared to a using a physical computer, is that the user's data, operating system, and internal computer components are now stored inside a virtual machine (VM) running in the IT central data center. A large scale hypervisor such as Microsoft Hyper-V Server is used to host the VM's.

VDI cannot be implemented by simply creating a large number of VM's, and making them available on the network. VM technology provides a number of benefits including cost savings by combining many desktop machines together.

Microsoft did not implement VDI as a single product because it is too large and complex. Instead, VDI is an umbrella term for many products working together. Applications may be delivered to users using any combination of RemoteApp, App-V, and MED-V, depending on the situation and the needs of the users.

These products allow system administrators to make applications available to users quickly, and allow them to resolve incompatibilities between applications and hardware – keeping users happy and productive. With these Microsoft products in place, VDI can now be implemented; application software need no longer be installed directly on user computers!

## Thin Client Computer Hardware

In a VDI world, all the data, application software and computing work is provided by the centralized servers. The user system supplies a remote desktop connection, and/or a web browser; it need provide nothing else. For this reason, the hardware does not need to be very fast or very powerful.

The picture below on the left shows a desktop thin client device that replaces the large box that is the heart of every computer. The picture on the right shows a mobile thin client device. Both are produced by Wyse Technology, one of several manufacturers of these specialty devices.

http://au.wyse.com/products/hardware/thinclients/Z90/index.asp

http://wyse.com/products/cloud-clients/mobile-clients/x90m7

Here is a comparison between a regular "fat client" against a typical thin client computer:

| Component | Typical Desktop PC | Wyse V30LE |
|---|---|---|
| CPU | Two (or more) core CPU | Single core 1.2 GHz CPU |
| RAM | 4 GB (gigabytes) and up | 512 MB (megabytes) |
| Monitor connectors | DVI or VGA | DVI, but able to support 2 monitors |
| Hard drive | 500 GB hard drive | 128 MB flash drive |
| DVD drive | Yes | None |
| USB ports | 6 | 3 |
| Power consumption | 150 watts | 13 watts |
| Price | $500 | $500 |
| Windows operating system | Included | Embedded into the firmware |

This table illustrates that a thin client computer is not very powerful; but since remote desktop places very low demands on the user's hardware, this is not a concern. In fact, there are very striking similarities between thin client computers and the ancient "dumb terminals" that were connected to large mainframe computers.

An alternative money-saving approach would be to use near-obsolete computers (that cannot meet the heavy demands of current application software) as the client systems.

Why would an enterprise purchase specially-built thin client computers when they are the same price as full desktop computers? One compelling reason is that they are very durable because there are no moving parts inside, such as a hard drive or a DVD drive. Regular computers and laptops suffer breakdowns and failures because of heat buildup or rough handling. Thin clients are designed to operate in harsh conditions such as factories, warehouses, and retail shops where dust, dirt, heat, and power fluctuations are common. The Mean Time Before Failure (MTBF) rating of the Wyse V30LE is 150,000 hours (17 years of continuous operation at 24 hours per day). The MTBF of a typical PC in the same work environment is 3 years.

A thin client device also uses far less power than a fat client PC. Therefore they are more environmentally friendly and cost less to operate.

Another advantage of VDI is that thin client computers are well-suited for handling highly sensitive data. In VDI, all the data stays in the data center; none of it is stored on the local machine. Therefore, if a thin client device is lost or stolen, there is no loss of confidential data.

Extended further, thin client computers do not need to be dedicated to specific end users; any user can use any thin client. When a user logs into a thin client, the VDI system will activate the correct VM for that user based on login ID. This is convenient for workers who wish to continue working from home after the end of the normal work day, or for mobile professionals switching between their office and mobile thin client computers.

However, virtualized desktop technology is not ideal for every user. Workers who place very heavy demands on the processing power of their systems should continue using dedicated physical computers. As with virtualized servers, hypervisors and other VDI components impose additional processing overhead on the servers to manage the many VM's in the system. The VMs, therefore, have poorer performance than equivalent physical equipment. For most users, the performance penalty is not noticeable (assuming that very powerful hardware is used to support VDI).

Another significant disadvantage of VDI is its dependence on the network infrastructure. If the network is having throughput problems (capacity) or is shut down, no one will be able to work.

# Lesson Summary

In this lesson, you explored some of the tools and features that allow an administrator to manage users and computers. You are now able to:

- ☑ Explain administrator and standard user accounts.
- ☑ Describe the function of the User Account Control feature and describe its prompts and elevation levels.
- ☑ Describe the process of local, network, and group policy application installation.
- ☑ Install and remove application software.
- ☑ Describe the function and characteristics of services, and identify startup types, service accounts and service dependencies.
- ☑ Describe the advantages provided by remote management tools.
- ☑ Explain the Microsoft Management Console (MMC) and create a custom console.
- ☑ Explain how group policy is useful for remote management.
- ☑ Describe Windows PowerShell.
- ☑ Describe the function of Remote Desktop and explain the necessary configuration settings and underlying technologies.
- ☑ Explain application virtualization and describe the features and functions of App-V, Remote Desktop Services, and RemoteApp.
- ☑ Explain Virtual Desktop Infrastructure (VDI).

**MMM**
Go online for Additional Review and Case Scenarios

# Review Questions

1. Amy is logged on as a standard user and begins to download and install a device driver. What will happen?
   a. The device driver will install successfully
   b. UAC will prompt for an administrator password
   c. UAC will ask if she wants to continue
   d. She will not be allowed to install the driver

2. Eloise is trying to run a program, but UAC displays a message that the program has been blocked by the system administrator. What should Eloise do?
   a. Click Yes to run the program anyway
   b. Enter an administrator password
   c. Contact the system administrator
   d. Try running the program from the command prompt

3. Dean is about to deploy an application to 5,000 users using Group Policy. What type of installation file must he place on the network share?
   a. a .MSI file
   b. a .msc file
   c. a cmdlet
   d. a .cpl file

4. Mike wants to create a custom MMC that he plans to use for monitoring system and application events. Which of the following snap-ins should he add to his console?
   a. Task Scheduler
   b. Performance
   c. Services
   d. Event Viewer

5. Thom is logged on as a standard user and is about to change his account password. What must he provide in order to successfully change his password?
   a. His current account password
   b. An administrator password
   c. A password reset disk
   d. He does not need to provide anything

# Lesson 4: Working with File Systems

## Lesson Objectives

In this lesson, you will learn how to manage and share files and folders. By the completion of this lesson, you will be able to:

- ☐ Explain disk partitions and logical drives.
- ☐ Describe the file systems supported in Windows 7, including FAT32 and NTFS.
- ☐ Describe how to format a drive and how to convert a drive from FAT32 to NTFS.
- ☐ Explain the purpose and function of HomeGroups and describe how to create and join them.
- ☐ Describe public shares, basic shares and advanced shares.
- ☐ Explain how to map network shares to drive letters.
- ☐ Describe share permissions, NTFS permissions and effective permissions.
- ☐ Explain how to share printers.
- ☐ Explain basic encryption concepts.
- ☐ Describe the function of Encrypting File System (EFS) and BitLocker, and describe how to manage encryption keys.
- ☐ Explain disk compression.
- ☐ Explain the function and characteristics of libraries and describe how to use, customize, create and delete libraries.

### Exam Objectives

4.1 Understand file systems
4.2 Understand file and print sharing
4.3 Understand encryption
4.4 Understand libraries
5.2 Understand storage

# Understanding File Systems

Objective 4.1 5.2

All storage media used for storing computer data includes a file system. That is, hard drives, CDs, DVDs, BDs, flash drives, tape drives and floppy drives all use file systems to store and organize data on the media.

The file system is actually the interface between the operating system and the storage drives on a computer. For example, when a program such as Microsoft Word needs to read a file from the hard disk, the operating system asks the file system to open the file.

A file system works as an index or database, and keeps track of the physical location of every piece of data stored on the media. It provides structure for organizing data and a method for referencing the location of the data. A file system also imposes certain constraints on files, such as setting a limit on the maximum file size or the length of a file name, or the number of files that may be stored.

Before investigating the specifics of file systems, you should be familiar with common terminology used in association with hard drives.

## Hard Drive Basics

Most PCs have one or more disk drives – devices that store information on a metal or plastic disk. A computer's hard disk drive stores information on a hard disk, usually located inside the system unit. The traditional hard disk is a rigid platter or stack of platters with a magnetic surface. Read/write heads in the disk drive are used to encode and read data on the hard disk surface.

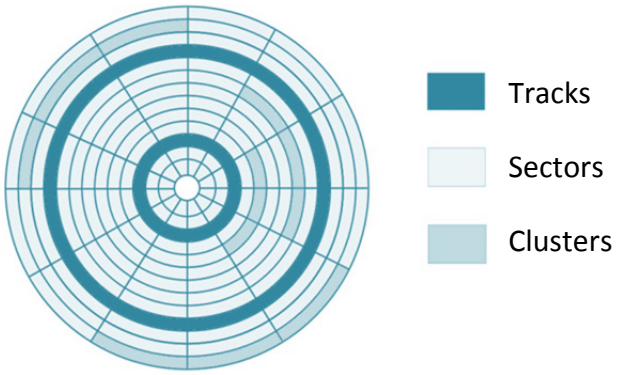
### Tracks and Sectors

Before data can be stored on a magnetic medium, the medium must be initialized or formatted. The hard disk manufacturer performs a low-level format which creates a set of magnetic concentric circles called tracks on each side of the disk. The number of tracks created varies depending on disk size as does the track density (the higher the density the more tracks that can be recorded on each platter). Each track is a separate circle numbered from the outermost circle to the innermost circle, starting with zero.

Each track is divided into sectors, which are the smallest units of data storage with which read/write heads can work. Each sector stores a fixed amount of user data. Traditional formatting provides space for 512 bytes or 2048 bytes of user data per sector. Newer hard drives used 4096 byte sectors.

Contiguous sectors are grouped into clusters. A cluster is a group of sectors used as the basic unit of data storage. File systems refer to clusters to identify the physical location of each piece of data on the disk.

### Hard Disk Drive Structure




## Partitions and Logical Drives

A hard disk needs to be partitioned and formatted before you can store data on it. A partition, sometimes also called a volume, is an area on a hard disk that can be formatted with a file system and identified with a letter of the alphabet (drive letter). For example, drive C on most Windows computers is a partition.

Even if you want to use only a single drive in the system, that drive must be partitioned before it can be recognized by the operating system. Many computers are partitioned as a single partition equal to the size of the hard disk. Partitioning a hard disk into several smaller partitions is not required, but can be useful for organizing data on the hard disk. For example, some users prefer to have separate partitions for operating system files, programs, and personal data.

There are two types of partitions you can create on a basic disk. These are:

| | |
|---|---|
| **Primary partition** | Can be used to start an operating system. A basic disk can contain up to four primary partitions, or three primary partitions and an extended partition with multiple logical drives. A primary partition is treated as a single logical drive. In Windows 7, if you use the Disk Management snap-in to create partitions, the first three partitions you create are primary partitions. If you require an additional partition, the fourth partition is created as an extended partition. |
| **Extended partition** | A container that can hold one or more logical drives. A hard disk can have only one extended partition. The extended partition itself is not formatted or assigned a drive letter. The logical drives created within the extended partition are formatted and assigned drive letters. A logical drive is technically not a partition (logical drives are created within the one allowable extended partition on a disk); but the operating system treats it in the same manner it treats a partition. Each logical drive is a volume, and is assigned its own drive letter. Logical drives function like primary partitions except that they cannot be used to start an operating system. |

If you partition a hard disk into multiple primary partitions, then you must identify one partition as the active partition. The active partition is read first at boot time. If no active partition exists, or if the operating system files are corrupted or missing, the computer will report error messages.

There can be only one active partition. In cases where the hard disk is partitioned into a single primary partition, then that partition is the active partition.

### Logical Drive Letters

The system drive will be identified as Drive C. Drive letters D through Z are available for assignment. Drives A and B can be used as drive identifiers for floppy disk drives only. Drive identifiers are also assigned to CD drives, DVD drives, and USB flash drives. They are also used to identify connections to network shares.

### Formatting

After you define a partition/logical drive, you must format it. The formatting process prepares the drive for use by the operating system; it creates the file system root directory and the files used to track the disk space (clusters) used for data storage. This type of formatting is known as high-level formatting.

## File Systems Supported in Windows 7

Windows 7 supports the following file systems for hard drives and removable storage media such as USB flash drives.

| | |
|---|---|
| **FAT12** | Used for floppy disks. When you format a drive smaller than 16 MB in Windows, it will be formatted as FAT12. |
| **FAT16 (or simply FAT)** | Supports partition sizes up to 4 GB. Used today to provide backward compatibility with older operating systems. To maintain compatibility with MS-DOS, Windows 95, and Windows 98, a FAT16 volume should not be larger than 2 GB. The maximum size for a single file is 2 GB. The root directory on a FAT16 volume can manage a maximum of 512 entries. Compatible with MS-DOS and all versions of Windows. |
| **FAT32** | Supports partitions up to 16 TB, and the maximum size for a single file is 4 GB. There is no limit on the number of root directory entries. Compatible with Windows 95 and later, as well as Windows NT 4.0 and later. Today FAT32 is most often used on USB flash drives. |
| **NTFS** | Can theoretically support up to 16 exabytes (1 EB = 1,000,000 TB). However, the current Windows design only supports partition sizes up to 256 TB, provided other supporting hardware and software such as the system BIOS are upgraded as well. File size is limited only by the size of the volume. Compatible with Windows NT 4.0 SP4 and later. Provides advanced features such as disk recoverability, compression, encryption and file-level permissions. |

**Note:** Different file systems are used on optical media, such as CDs, DVDs and BDs. One of the oldest optical media file systems is Compact Disc File System (CDFS). Today, most optical media uses the Universal Disk Format (UDF) file system.

## File Allocation Table (FAT) File System

File Allocation Table (FAT) is a file system that uses an index table, called the FAT table, for tracking the location of data on the disk. Specifically, the FAT table tracks cluster use. The table contains entries for each cluster of disk storage, and two copies of the FAT exist on each volume for the sake of redundancy.

Each cluster on the drive is identified in the FAT as:

- Unused
- In use by a file
- Bad cluster
- Last cluster in a file

Entries for clusters that are in use by a file include the number of the next cluster in a file, or a marker that indicates the end of the file.

For example, suppose you want to open a file named README.txt on the hard drive. The root file directory of the disk contains the number of the first cluster of the README.txt file. The operating system then examines the entries in the FAT table looking up the cluster number of each successive part of the README.txt file as a cluster chain until the end of the file is reached. Once all the clusters have been identified, the file is loaded into memory and displayed.

The FAT file system was first developed in the late 1970s, when the size of storage media was relatively small. As the size of hard disks has increased over the years, so has the number of bits required to identify every cluster in the FAT table. Consequently, several versions of FAT have evolved, each using a different number of bits for identifying clusters in the FAT table. For example, FAT12 (which uses 12 bits for each element in the FAT table) is still used for floppy drive media, while FAT16 and FAT32 (which use 16 bits and 32 bits, respectively) are used for portable high-capacity storage devices such as USB flash drives.

Each successive standard supports larger hard disk drives and larger file sizes. As the FAT standard has expanded, backward compatibility with older operating systems has been preserved.

### Uses

FAT is still widely supported by most PC-based operating systems and embedded operating systems, and is the default file system for removable media (except for optical media such as CDs and DVDs); thus, it is commonly found on floppy disks, memory cards, USB flash drives, PDAs, digital cameras, and mobile phones.

Up through Windows ME, FAT was also commonly used on hard disks. On Windows systems, however, its use has declined since the introduction of Windows XP, which primarily uses the newer NTFS format.

The main reason to format a hard disk or partition with FAT32 today is to support a multiboot configuration that includes Windows 95, Windows 98, or Windows Millennium Edition in addition to Windows 7. A multiboot configuration allows you to install more than one operating system on a computer, and select which one you want to use when you boot up the system.

To set up a multiboot configuration that includes one of these earlier versions of Windows, you need to install the earlier operating system on a FAT32 (or FAT16) partition and ensure that it is a primary partition. Any additional partitions that you need to access when using the earlier versions of Windows must also be formatted using FAT32.

## New Technology File System (NTFS)

New Technology File System (NTFS) is an advanced file system proprietary to Windows NT/2000/XP/Vista and Windows 7. It supports extremely large volumes, file-level security, compression, encryption and auditing.

Instead of an index table, NTFS maintains a database of information about files stored on the volume. This database is called the Master File Table (MFT). An MFT record for a particular file includes information about the following:

- File size
- Time and date stamp
- Data content
- Permissions

Two copies of the MFT are maintained on each volume – one is stored at the beginning of the volume and one is stored in an alternate location. By default, 12.5 percent of the volume space is reserved for the MFT, which helps prevent fragmentation of the MFT itself.

NTFS is a 64-bit file system. That means 64-bits are used for elements in the MFT, allowing NTFS to manage extremely large volumes and support individual files of tremendous size.

> The fact that NTFS uses a 64-bit structure for tracking and managing files on disk in no way constrains its use to 64-bit editions of Windows. NTFS can be used in both 32-bit and 64-bit editions.

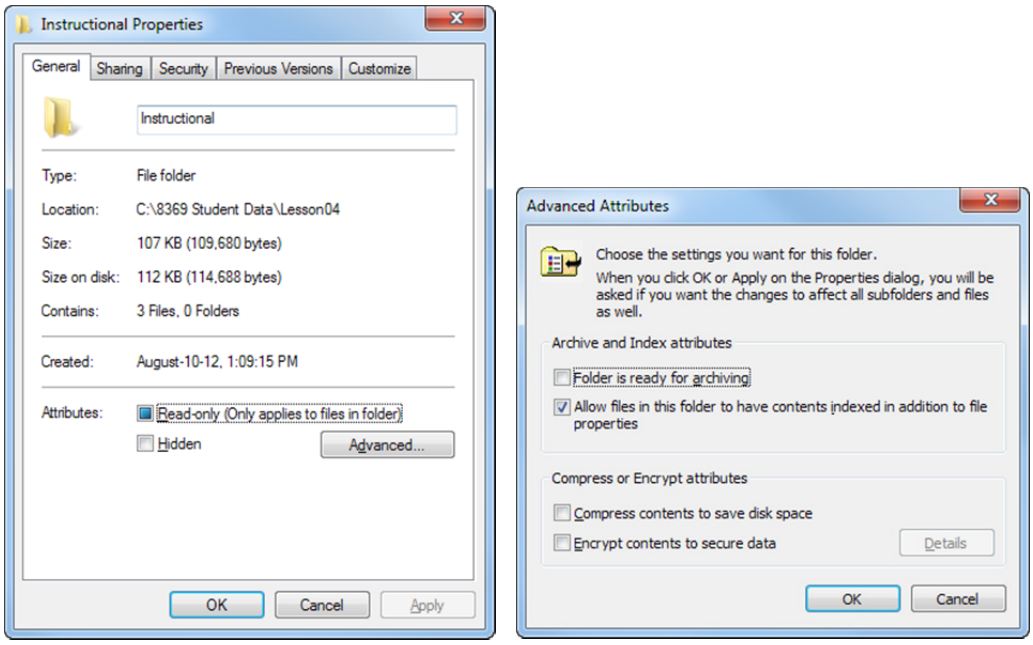
### NTFS Versus FAT32

NTFS is the preferred file system for Windows 7. It has many benefits over the earlier FAT32 file system, including:

- The ability to recover from some disk-related errors automatically.
- Improved support for larger hard disks.
- Better security because you can use permissions and encryption to restrict access to specific files for certain users.

One of the primary benefits of an NTFS file system is that it allows you to secure resources. NTFS allows you to set *permission bits* on system resources (for example, files and directories). With NTFS, you can protect files so that only certain users or groups of users can read them. One group of users may be able to execute applications in a directory, whereas another group may have full access to all the files within that directory.

Files and folders on an NTFS volume include a Security tab in the Properties dialog box, and allow you to specify either compression or encryption as advanced attributes. Click the Advanced button in the Attributes section of the General tab to open the Advanced Attributes dialog box.




FAT32 doesn't have the same security-related features as NTFS, so if you have a FAT32 hard disk or partition in Windows 7, anyone who has access to your computer can read any file on it.

A drawback of NTFS is its overhead – it does not perform well on small volumes.

## Formatting Drives

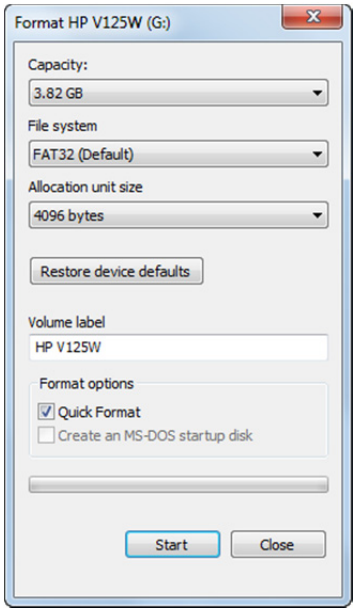
Generally, you need to format a drive only when adding storage such as a new hard drive to a computer. However, you can format removable media as well.

For example, you could format a USB drive at the command prompt using the following command:

Format *volume* /FS:*filesystem*

Replace *volume* with the letter of the drive you want to format, and replace *filesystem* with the file system you want to use, such as NTFS, FAT32, FAT.

You can also format a volume from Windows Explorer or from the Disk Management snap-in.



## Converting the File System

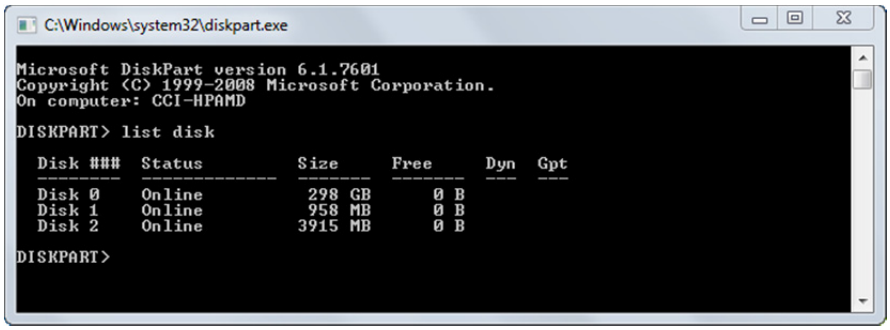
You can use the convert utility to convert a partition or logical drive from FAT32 into NTFS . You can run the Convert utility from the command prompt using the following syntax:

convert *volume* /FS:NTFS

Replace *volume* with the letter of the drive you are converting into NTFS. Note that you can't use the utility to convert a partition or drive from NTFS to FAT32; you must use the format utility.

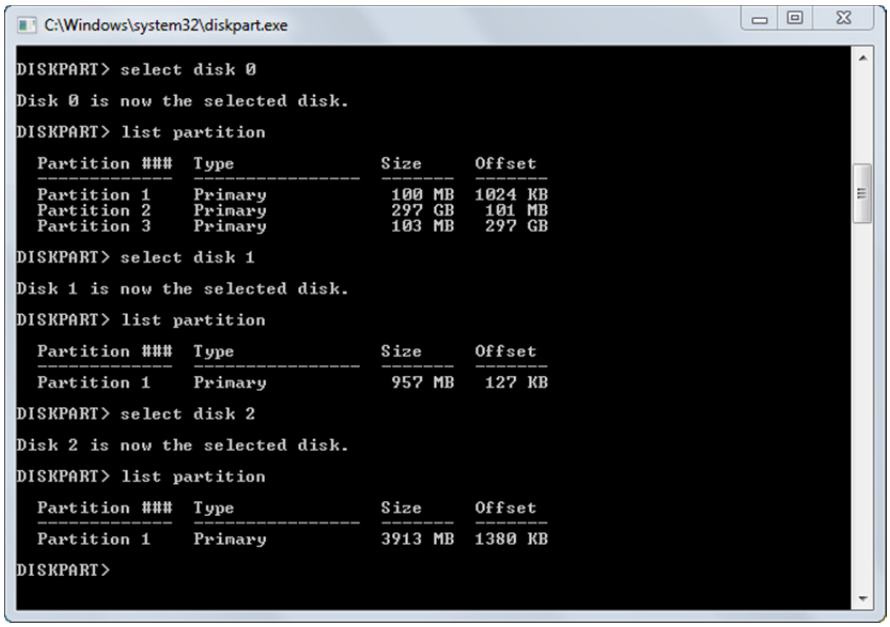
## Viewing Disks, Partitions, Volumes and File Systems

Windows 7 provides several utilities you can use to view and manage disks and file systems. For example, the Diskpart list disk command will show how many physical disks are installed.



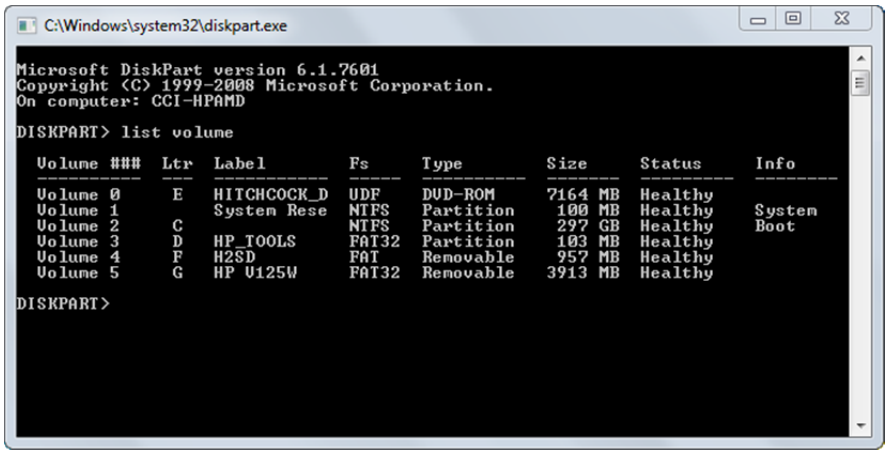

The system shown in the figure contains three disks. On the system shown in the figure, Disk 0 is a 300 GB hard disk, Disk 1 is a 1 GB SD memory card, and Disk 2 is a 4 GB USB flash drive. (Note that optical media is not represented as a disk.)

You can view the partitions on a disk by selecting the disk and using the list partition command.




Disk 0 has three primary partitions, Disk 1 and Disk 2 are each a single primary partition.

You can also use the Diskpart list volume command to display the volumes on the system.



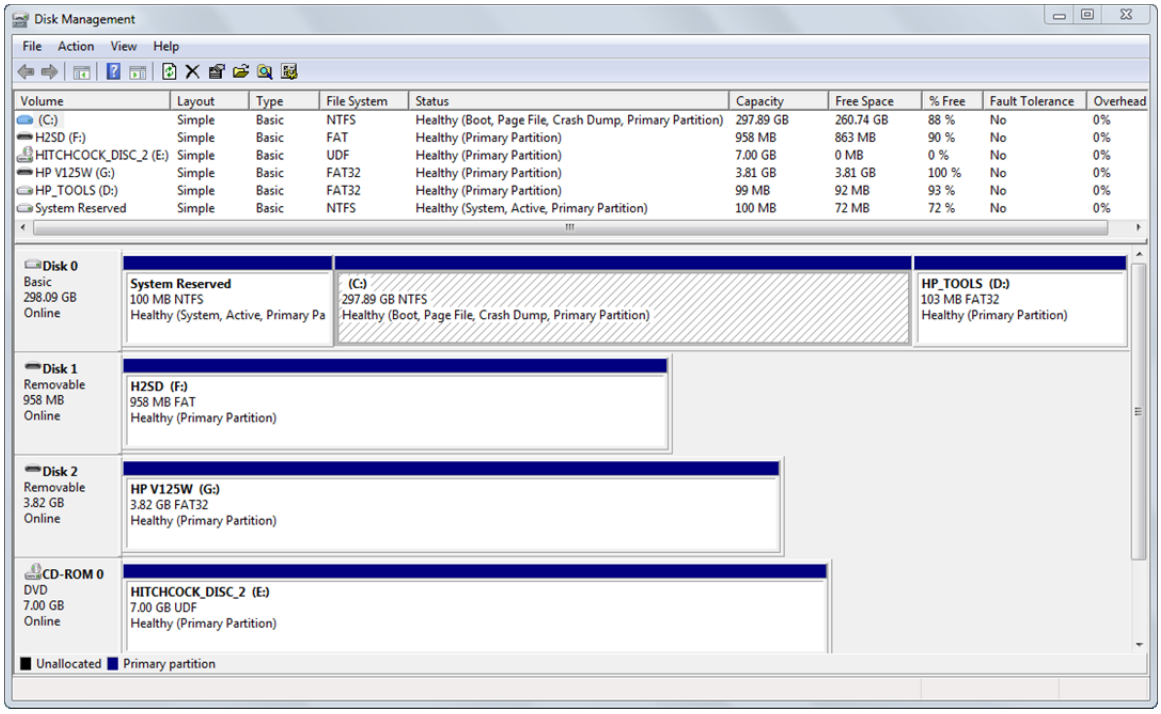

The list volume command shows all the volumes on the system, including those on optical media.

By comparing partition and volume size between the two figures, you can determine that the three partitions on the hard drive are:

- Volume 1 (a reserved 100 MB partition that has not been assigned a drive letter) – This volume is created during Windows 7 installation. Because it is not assigned a drive letter, users cannot accidentally access this volume and write or remove files on it.
- Volume 2 (the C: drive)
- Volume 3 (the D drive)

Additionally, Volume 4 is the SD memory card (Drive F); Volume 5 is the USB flash drive (Drive G); and Volume 0 is a DVD (Drive E).

You can also use the Disk Management snap-in for a graphic view of the disks, partitions and volumes on a system.




Notice that in the figure, the active partition is the 100 MB partition reserved by the operating system. When Windows 7 is installed, it creates and reserves this 100 MB partition for BitLocker information and files required for booting a system with an encrypted system drive. (You will learn about BitLocker and encryption later in this lesson.)

You can also use the Disk Management snap-in to format drives.

## Exercise 4-1: Working with File Systems (Instructor-led demo)

In this exercise, your instructor will demonstrate how to view disks and volumes, explore properties, and convert a file system.

*A USB flash drive formatted with the FAT32 file system is required to perform the steps of this exercise.*

First, you will view disks, volumes and file systems using the diskpart utility.

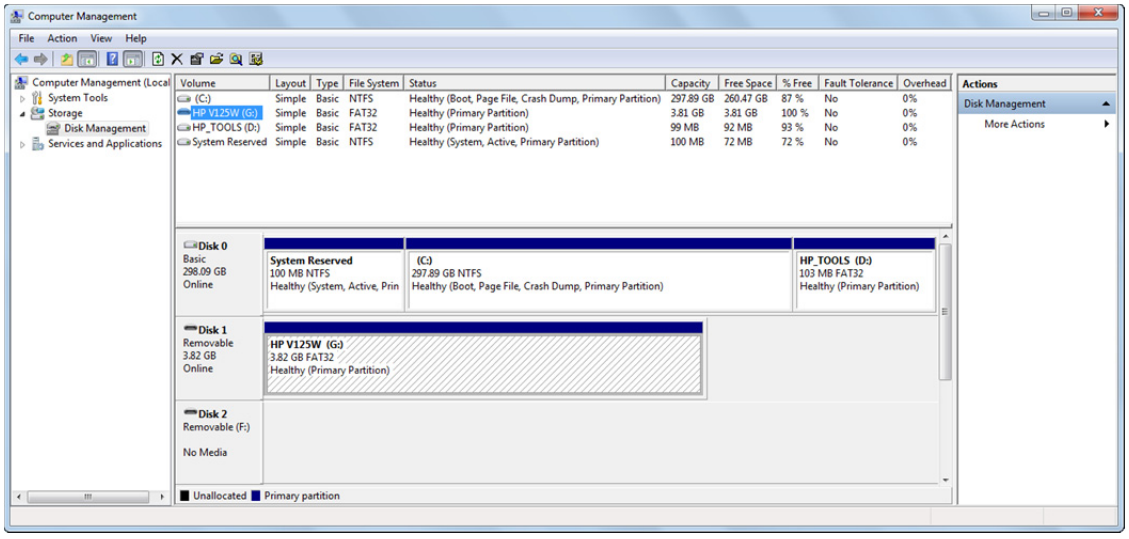
1. Log on to the system if necessary using an administrator account.
2. Insert a USB flash drive into an open USB port on the system. If the AutoPlay window appears, close it.
3. Click the **Start** button, type: `Diskpart` in the Search box, then press ENTER to start the Diskpart utility and click **Yes** if prompted by the User Account Control.
4. At the diskpart prompt, type: `help` and press ENTER to view a list of all the available commands.
5. At the diskpart prompt, type: `list` and press ENTER to view the options that are available for the list command. Note that you can list disks, partitions, volumes or virtual disks.
6. Type: `list disk` and press ENTER. Can you identify the hard disk and the USB flash drive in the list disk output? Are there additional drives on the system?
7. Type: `list volume` and press ENTER to see the volumes on the system. Record the volume number, drive letter, label, and file system for each volume in the table provided.

| Volume | Letter (Ltr) | Label | File System (Fs) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

8. Type: `exit` and press ENTER to exit the diskpart utility.

Next, you will identify file systems in the Disk Management snap-in.

9. Click the **Start** button, then right-click **Computer** and select **Manage** to open the Computer Management Console.
10. In the console tree, expand the **Computer Management** node if necessary, expand the **Storage** node, then click **Disk Management**.
11. In the display area, click the various volumes and notice which sections are highlighted in the disk detail section at the bottom of the window. Which file systems are in use? Does the system include a partition (with a volume name such as Tools or Factory Image) that was added by the system manufacturer? If so, what file system is used on that partition? Why do you think that particular file system was chosen?



12. Close the Computer Management Console.

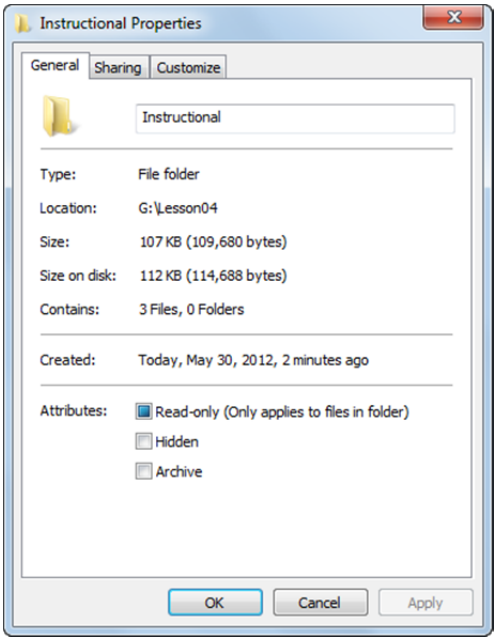
Next, you will view disk information using Windows Explorer.

13. Right-click the **Start** button, then click **Open Windows Explorer**.
14. In the navigation pane, right-click the USB flash drive and select **Properties**. Notice that the volume label, drive letter and file system are indicated on the General tab of the Properties dialog box.
15. Close the Properties dialog box.

Next, you will copy files to the flash drive and inspect a few properties.

16. In the navigation pane, click **Desktop**, double-click the *Student Data* folder in the contents pane, right-click the *Lesson04* folder, then select **Copy**.
17. In the navigation pane, click the flash drive, right-click in an empty area in the contents pane, then select **Paste** to copy the *Lesson04* folder to the flash drive.
18. In the contents pane, double-click the *Lesson04* folder, right-click the *Instructional* folder and select **Properties**.

    Note the three tabs that are available for the folder: General, Sharing, and Customize. The Security tab is not available. On a FAT32 volume, there are no security options available. Notice also that there is no Advanced button in the Attribute section of the dialog box. On a FAT32 volume, you cannot set attributes for compression or encryption.



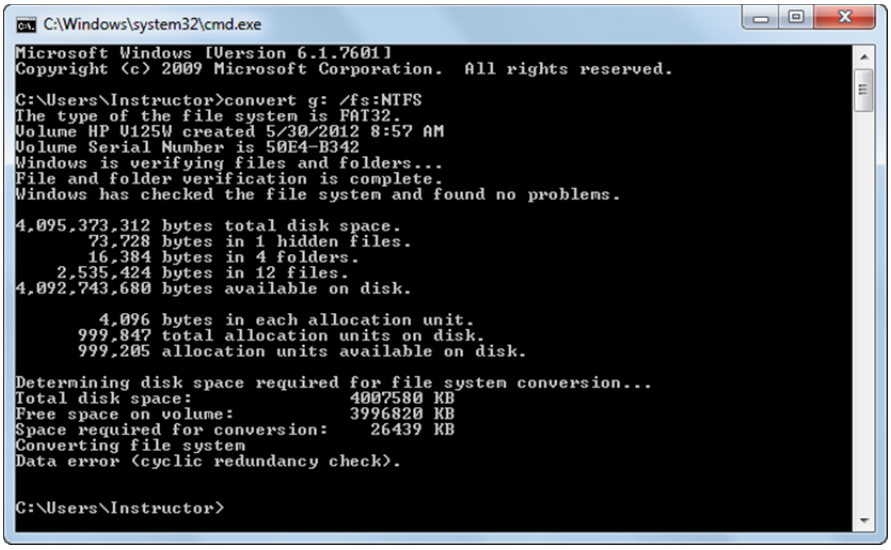

19. Close the Properties dialog box, then close Windows Explorer.

Next, you will convert the file system on the flash drive from FAT32 to NTFS. This exercise is for demonstration purposes only. Normally, you would convert a hard drive partition, as flash drives function very well with the FAT32 file system.

20. Open a command prompt window.
21. Type the following command substituting the drive letter for the USB flash drive for the *<drive letter>* parameter:

```
convert <drive letter>: /fs:ntfs
```

22. Press ENTER to convert the volume.




23. When the conversion is complete, open the diskpart utility again and use the list volume command to confirm that the file system on the flash drive is now NTFS.
24. Exit the diskpart utility and close the command prompt window.

Finally, you will view the file and folder properties available on an NTFS volume.

25. Open Windows Explorer, navigate to the flash drive, and open the *Lesson04* folder. Notice that all the data on the flash drive remains intact. Converting from FAT32 to NTFS does not destroy any data.
26. Right-click the *Instructional* folder, then select **Properties**.

    Now there are four tabs in the Properties dialog box: General, Sharing, Security and Customize. Notice also that the Advanced button displays in the Attribute section of the dialog box. (You will explore the advanced options later in this lesson.)
27. Close the Properties dialog box for the folder, then close Windows Explorer.

In this exercise, you viewed disks and volumes, explored properties, and converted a drive from FAT32 to NTFS.

# Setting Up File and Print Sharing

Objective 4.2

One of the primary reasons for participating on a network is to share files and resources. Windows 7 computers can participate in three types of networks:

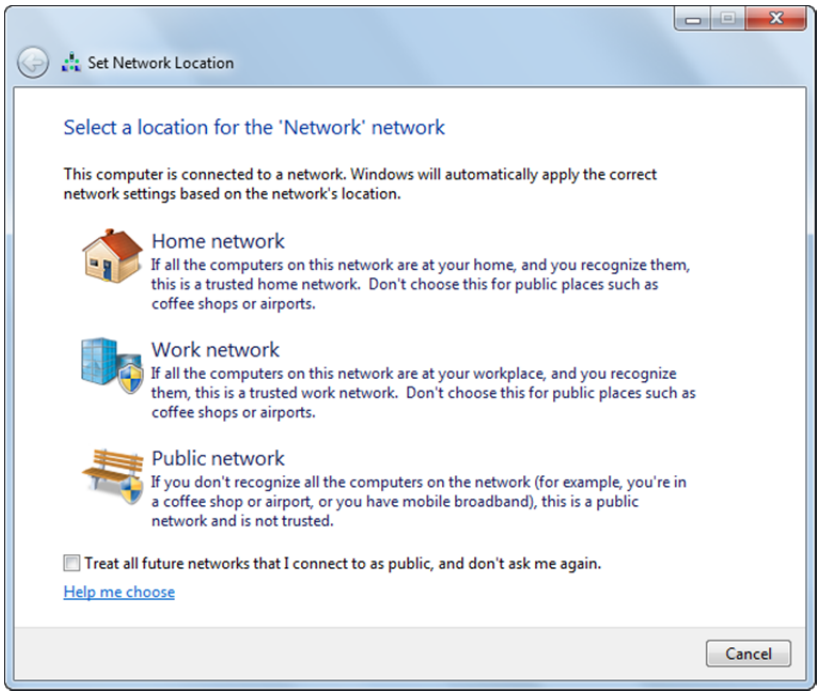
| | |
|---|---|
| **Workgroup** | This type of network can include systems running various versions of Windows. A workgroup is not protected by a password, and each computer in the workgroup has a local set of user accounts. In order for a user to access resources on a target machine, that user must have an account on that target machine. All systems in the workgroup must be on the same network and have the same workgroup name. |
| **HomeGroup** | Can include only Windows 7 systems. A HomeGroup is protected by a password, but users need not have an account on a target machine within the HomeGroup in order to access resources on that target machine. |
| **Domain** | Requires a domain controller (a server that manages and authenticates users) which runs a server operating system. A user must have an account in Active Directory in order to log on to a domain-joined computer. |

# HomeGroups

The easiest way to share files on Windows 7 client systems on a network is to create or join a HomeGroup. (Note that HomeGroups are not available on Windows Server 2008 R2.)

A HomeGroup enables you to share documents, music, pictures, videos and printers between networked computers at home or in a small business without using a server. All computers in the HomeGroup must be running Windows 7. By default, the documents, music, pictures and videos folders in Windows 7 are arranged into structures called libraries. You will learn about libraries later in this lesson. For now, it is sufficient to understand that you may see references to "libraries" in the Windows help documentation concerning HomeGroups.

If you have Windows 7 and your system detects a new network connection (e.g. new computer started up for the first time or you start up your laptop at the local coffee shop), you are asked to specify the type of network to which you are connected – Home network, Work network or Public network.




**MMM**
Working with HomeGroups

The Home network option is intended for use in a home environment where all computers are operating in a trusted network. That is, it is protected from the Internet by a residential gateway (router with a hardware NAT firewall), but the HomeGroup enables users to access shared libraries on the other computers as easily as on their own computer. The Work network option is intended for computers in a work environment, and security requirements are higher than a home network even though it is a trusted network. In this network, you must have your account created on a target machine before you are allowed to access its files, whether you are logging on directly onto that computer or through the network. If you are using your computer at a local coffee shop offering free wifi, you should select the Public network to prevent other computers that are sharing the same wifi connection from accessing the files on your computer.

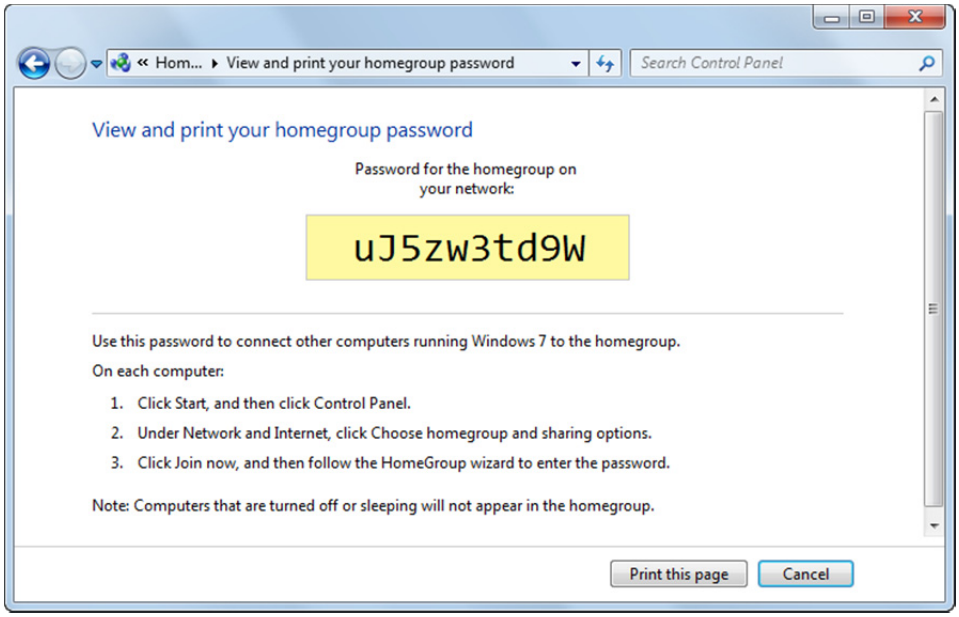
If you select Home network and a HomeGroup does not already exist on your network, you will be prompted to create one. If a HomeGroup does exist, you will be asked if you want to join it.

When you join a HomeGroup, you specify which folders or libraries you want to share. Windows 7 automatically shares your Pictures, Music, and Videos libraries. You can check or clear boxes to specify more or fewer. You can also specify to share your printers.

Libraries are available in all editions of Windows 7; however, in Starter and Home Basic editions you can join a HomeGroup but not create one. Computers that belong to a domain can join a HomeGroup but they can't share files. These systems, can however, access files shared by others in the HomeGroup.

HomeGroups are protected by a password, and you must know the HomeGroup password before you can join. You can display and print the HomeGroup password on the system that originally created the HomeGroup, or on any system that has subsequently joined the HomeGroup.

To view and print the HomeGroup password, open the Control Panel in either Large or Small icons view, then click the **HomeGroup** link, then click the **View or print the homegroup password** link to open the View and print your homegroup password page.

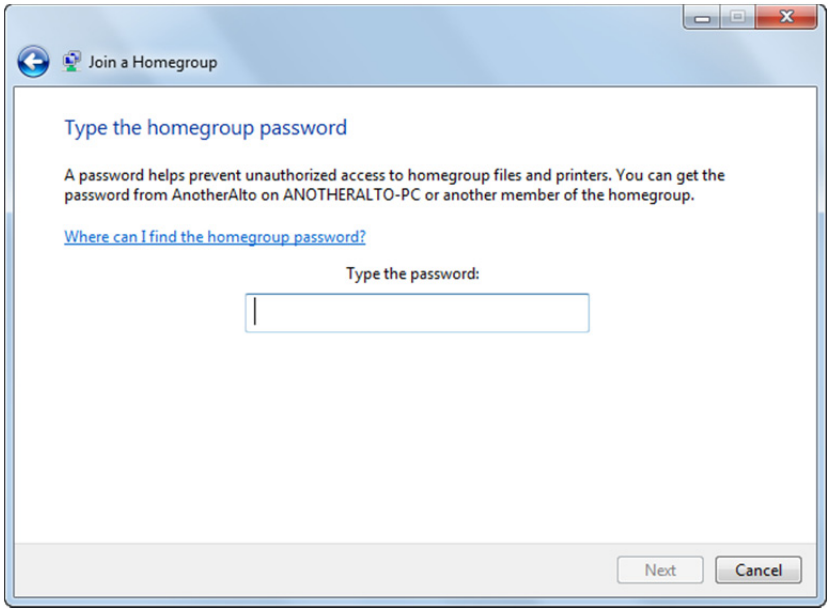



## Joining a HomeGroup

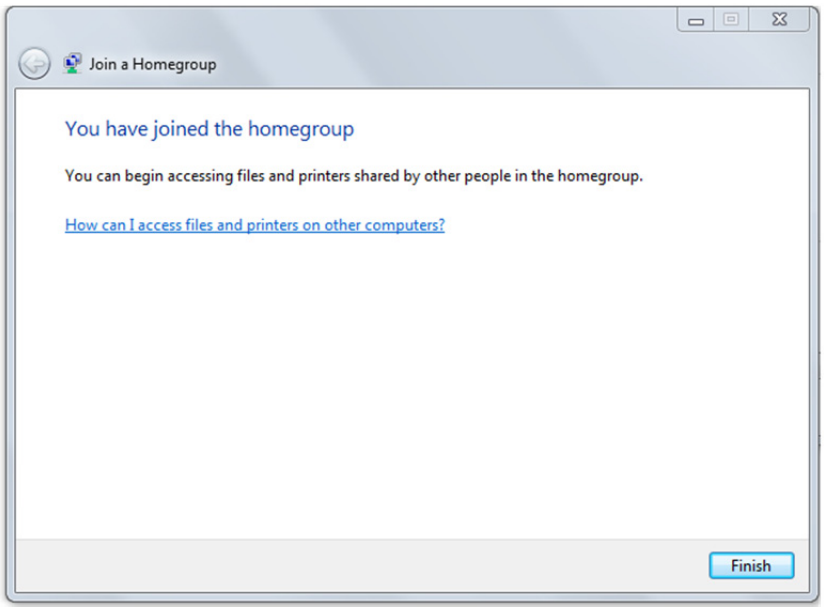
When you are prompted to join a HomeGroup on your network (or when you click the HomeGroup link in the Control Panel before you have joined a HomeGroup), the HomeGroup page appears.

Click the **Join now** button to open the Join a HomeGroup dialog box.

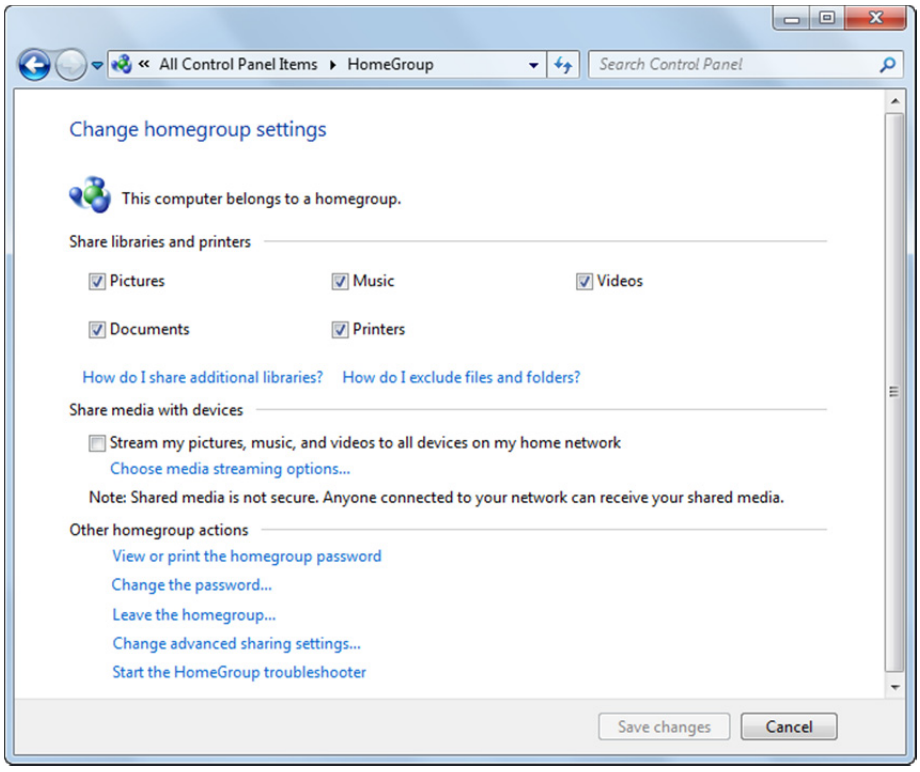

Select or clear the checkboxes for the libraries/printers that you want to share, then click **Next**.



Enter the HomeGroup password, then click **Next**. When you have successfully joined the HomeGroup, click **Finish**.

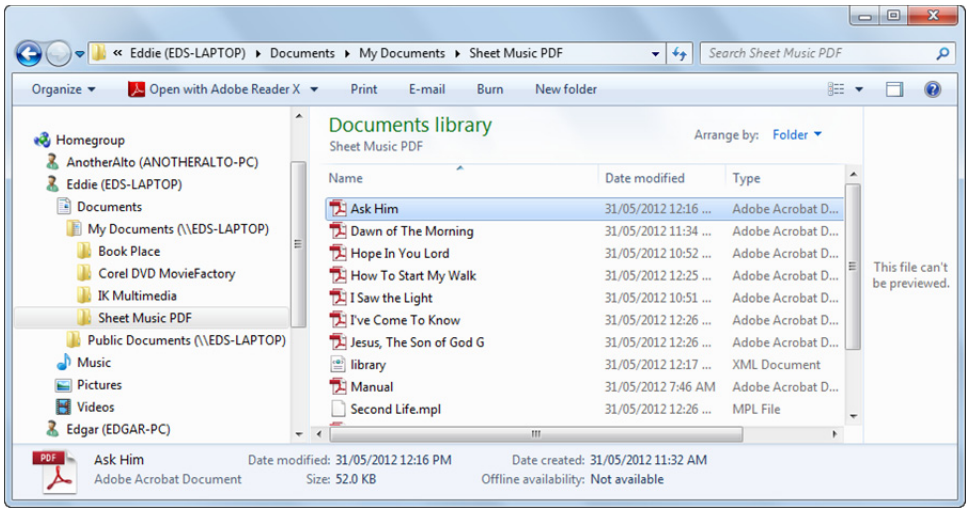



Once a system belongs to a HomeGroup, you can adjust the HomeGroup settings in the HomeGroup page of the Control Panel.



## Accessing HomeGroup Files

Once you have joined a computer to a HomeGroup, other HomeGroup computers appear in Windows Explorer under the HomeGroup heading. You can navigate the shared libraries on the HomeGroup computers just as you can local folders.




## Controlling What is Shared

When you join a HomeGroup, libraries are initially shared with Read access – other people can look at or listen to what is in the library, but can't make changes to the files in it. In order to make changes to files, or to paste copied files onto another system, a user must have Read/Write access.

You can control which specific files and folders are shared, and you can control the level of access using the Share with menu. The Share with menu can be used to control how files and folders are shared both within a HomeGroup, and outside a HomeGroup.

To control sharing and the level of access, open Windows Explorer, select the item you want to configure, click **Share with** in the toolbar, then in the shortcut menu:

- To prevent the item from being shared, click **Nobody**.
- To share the item with some people but not others, click **Specific people**, select each person you want to share with, then click **Add**. Click **Share** when you are finished.
- To change the level of access, select either **Homegroup (Read)** or **Homegroup (Read/Write).**

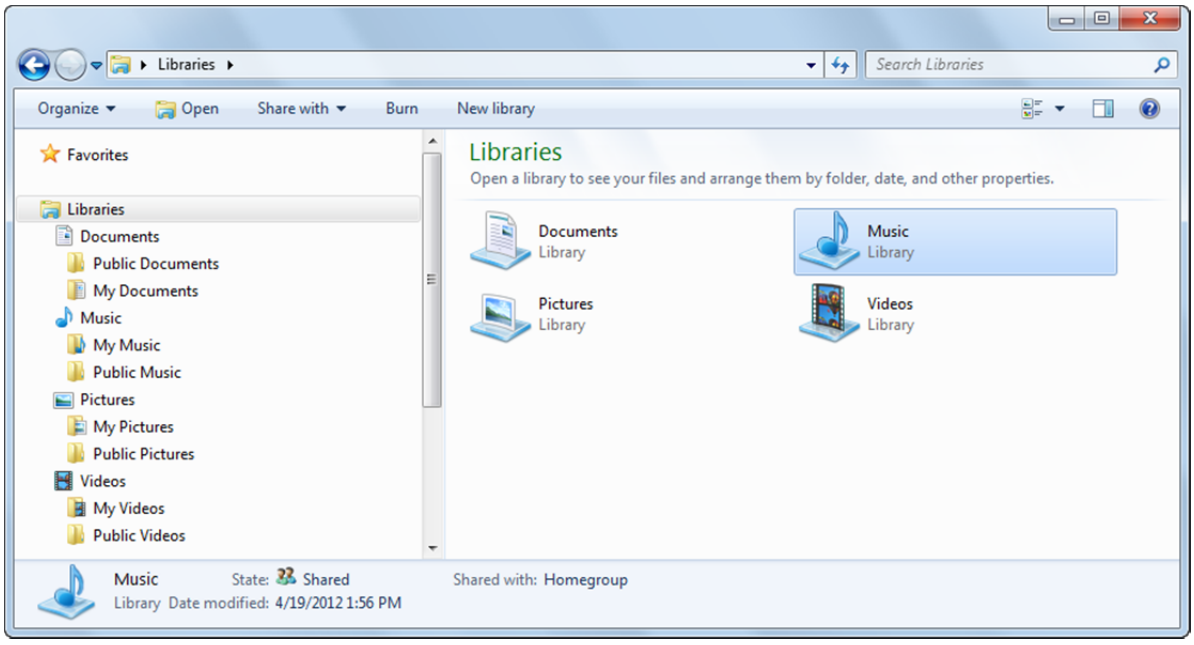
You will learn more about using the Share with menu in the next section.

# Setting Up Shares

You create network shares to allow users to access local resources across the network. A share is a shared folder; that is, it is a folder that has been configured to be available to other users on the network. There are four share types you can create: public, basic advanced, and hidden.

## Public Shares

Public shares are the Public folders in each of the four default Windows libraries. These are the Public Documents, Public Music, Public Pictures and Public Videos folders, and they are pre-configured to be shared.

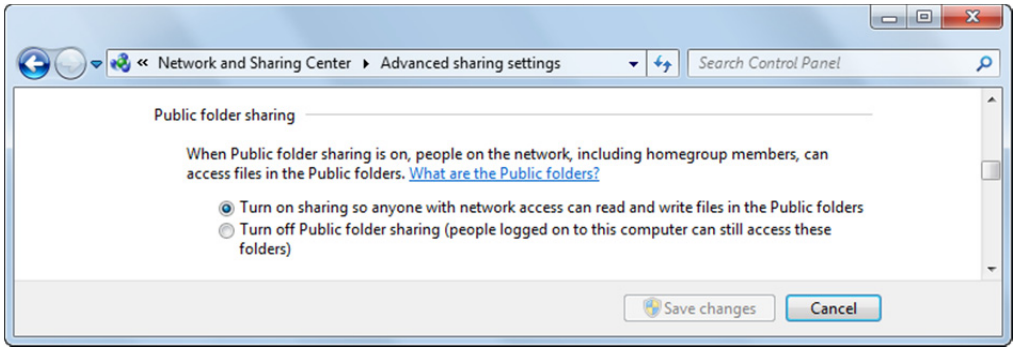



When you copy a file or folder into a public share, that file or folder becomes immediately available to other users on your computer or other people on your network.

Any file or folder you put in a public folder is automatically shared with people who have access to your public folders. You cannot restrict people from seeing or updating files in a public folder; that is, they can not only open and read those files, but they can also modify or delete them. It is an all-or-nothing proposition.

Public folder sharing is turned off by default, except on a HomeGroup. When public sharing is turned on, anyone on your computer or network can access your public folders. When public sharing is turned off, only people with a user account and password on your computer have access.

If you need to turn on public folder sharing, open the Control Panel, open the Network and Sharing Center, then click the **Change advanced sharing settings** link to open the Advanced sharing settings page. Expand your current network profile if necessary, scroll down to the Public folder sharing section, then select **Turn on sharing so anyone with network access can read and write files** in the Public folders.

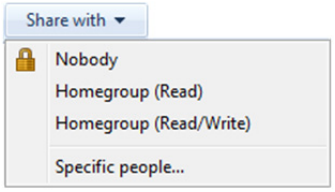



You can limit public folder access to people with a user account and password on your computer by turning on Password protected sharing (also found on the Advanced sharing settings page).

## Basic Shares

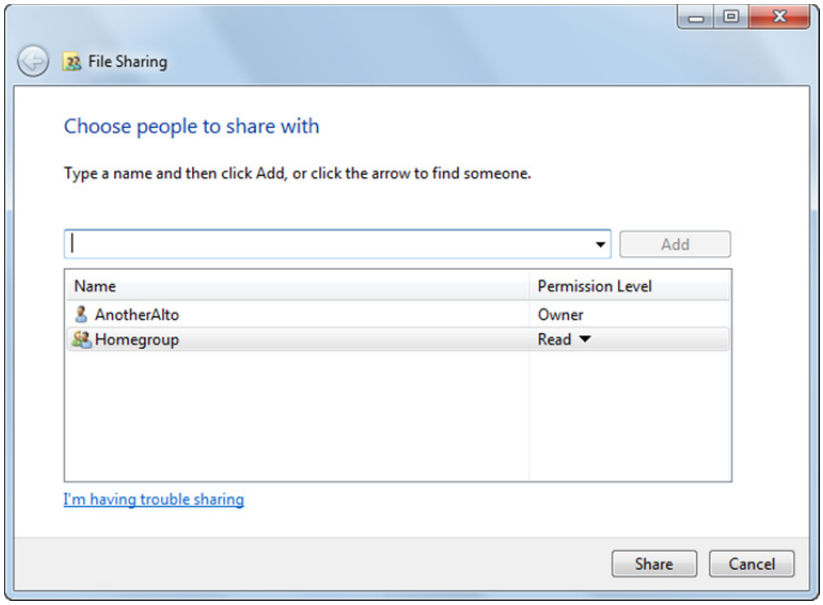
You can share individual files and folders (that are not in a Public Folder) and exercise a degree of control over the type of access granted by creating a basic share. To create a basic share, select an option in the Share with menu. In Windows Explorer, select the item you want to share, then click **Share with** in the toolbar.

You can select from the following options:




| | |
|---|---|
| **Nobody** | Does not share the item, or stops sharing an item that was previously shared. |
| **Homegroup (Read)** | Shares the item with your entire HomeGroup, but people in the HomeGroup can only open the item; they can't modify or delete it. |
| **Homegroup (Read/Write)** | Shares the item with your entire HomeGroup and lets them open, modify or delete it. |
| **Specific people** | Opens the File Sharing wizard, which allows you to select individual people with whom to share the item. |

You can use the File Sharing wizard to select specific people with whom to share files and folders. Click the arrow next to the text box, select a name from the drop-down list, then click the **Add** button.

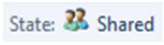



After you have added a name to the list, click in the Permission Level column and select the type of permission you want to grant. Your options are:

- **Read** – recipients can open, but not modify or delete the file
- **Read/Write** – recipients can open, modify or delete the file

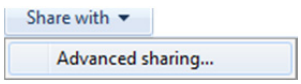
When you have finished adding people, click the **Share** button.

In Windows Explorer it is easy to tell which items are shared and with whom. Select an item in the contents pane, then look at the details pane. The state of the selected item indicates whether it is shared.




You can point to the state indicator and a pop-up box will display the names of the individuals or groups with whom the item is shared.

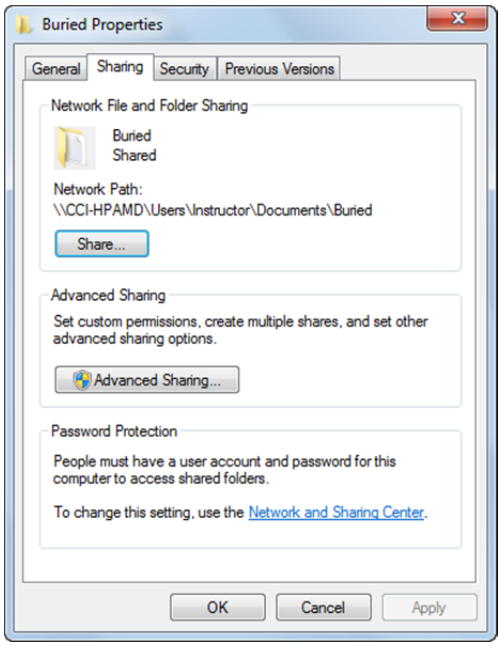
Note that there are some locations in Windows that can't be shared directly using the Share with menu. For example, you cannot share your entire C: drive in a basic share. When you try to share locations such as these, the Share with menu displays only one option: Advanced sharing.




Click the **Advanced sharing** button to create an advanced share, which you will read about in the next section.

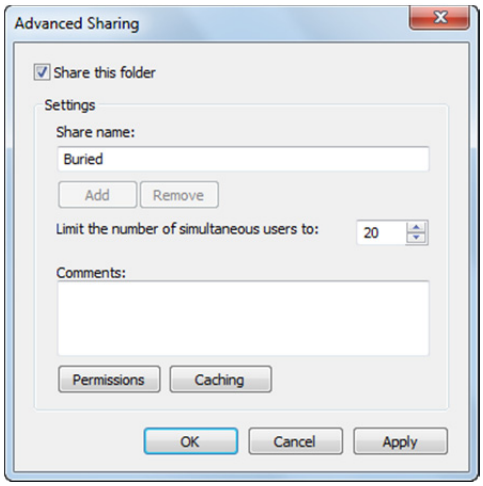
## Advanced Shares

Advanced shares allow you to set permissions on a share with more granularity than on a basic share. To create an advanced share, right-click the file or folder, then select **Properties** to open the Properties dialog box. Click the **Sharing** tab.

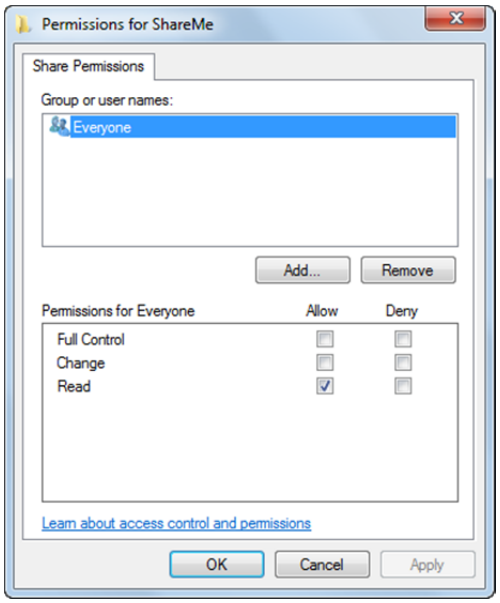



Clicking the **Share** button will open the File Sharing wizard, which you can use to create a basic share. Click the **Advanced Sharing** button to open the Advanced Sharing dialog box.

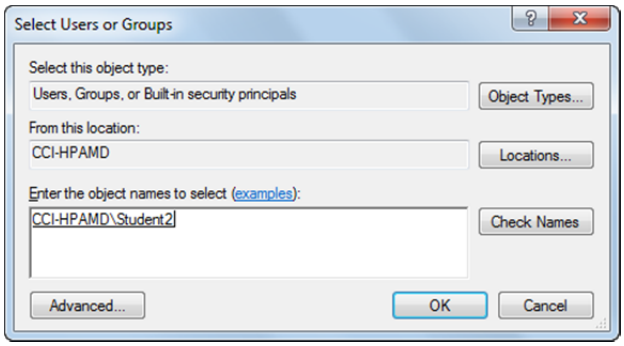
In the Advanced Sharing dialog box, select the **Share this folder** check box. You can accept the suggested share name or type a new name for the share.



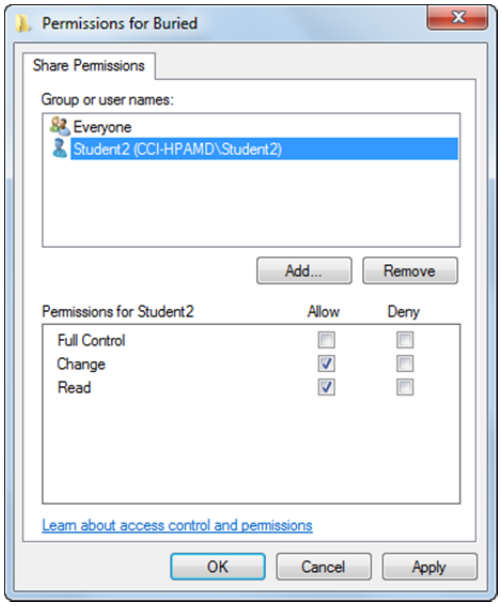

To specify users or change permissions, click the **Permissions** button.




By default, everyone will have the ability to read files on the share if you turn on sharing for those files or folders. Click the **Add** button or the **Remove** button to add or remove specific users or groups.




Enter the name of the user or group you want to share with, then click **OK** to add the user or group and return to the Share Permissions page.



On the Share Permissions page you can select check boxes for the permissions you want to assign. When you are finished, click **OK** to close the Share Permissions page, click **OK** to close the Advanced Sharing dialog box, then click **Close** to close the Properties dialog box.

## Hidden Shares

You can create a hidden shared folder by appending a '$' to the end of the share name. When you use this technique, other users will not see the share name displayed when they use Windows Explorer or the Net View command to list the shares that are accessible on a server. To open this hidden share, you must enter the full UNC (see Mapping Drives below) with the '$' at the end; for example:

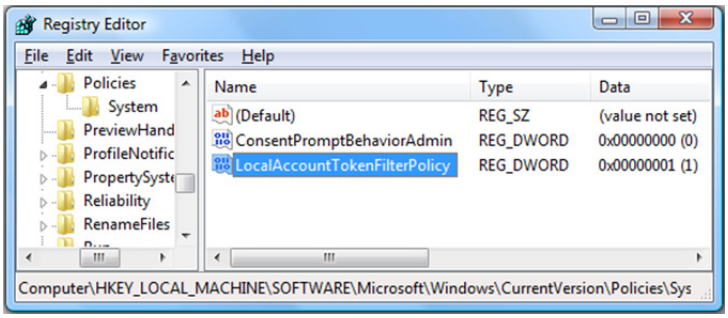
```
\\ANOTHERALTO-PC\Users\AnotherAlto\Documents\ShareMe$
\\ANOTHERALTO-PC\C$
```

This feature is commonly referred to as administrative shares because it is typically used by system administrators to access the C: drive (or any other volume) directly at the root directory on the many servers that they manage. It is poor security practice to allow users to have access to the root directory of any server, so the share is hidden and the permissions are set to permit access only to system administrators. The term administrative share is actually a misnomer because non-administrative access privileges can be assigned instead of allowing full control. Hidden shares can be set up on any folder in the folder hierarchy on any drive volume.

With the introduction of stronger security in Windows Vista and then Windows 7, this feature has been disabled by default on any computer that is not joined to a domain. To enable it manually on a computer that is in a Workgroup network (i.e. not part of a domain and has only local user accounts), you must use regedit and navigate to the following:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

You must then add a new 32-bit DWORD key named `LocalAccountTokenFilterPolicy` and set the value to 1.




If you want to disable hidden shares, you can set the value to 0 (zero) or delete the key. (You will learn more about the Windows Registry in Lesson 6.)

To ensure that file sharing will work, you must also verify that the File and Printer sharing option is turned on:

1. Open the Control Panel and select **Network and Internet**.
2. Open the **Network and Sharing Center**.
3. Click **Change advanced sharing settings**.
4. Open the Home or Work network profile, and turn on the File and Printer sharing option.

Finally, you must ensure that the computer is not connected to a HomeGroup. If the computer is connected, you can open hidden shares on other computers but others cannot access hidden shares set up on this computer.

1. Open the Control Panel and select **Network and Internet**.
2. Open the **HomeGroup**.
3. Click **Leave the homegroup**.

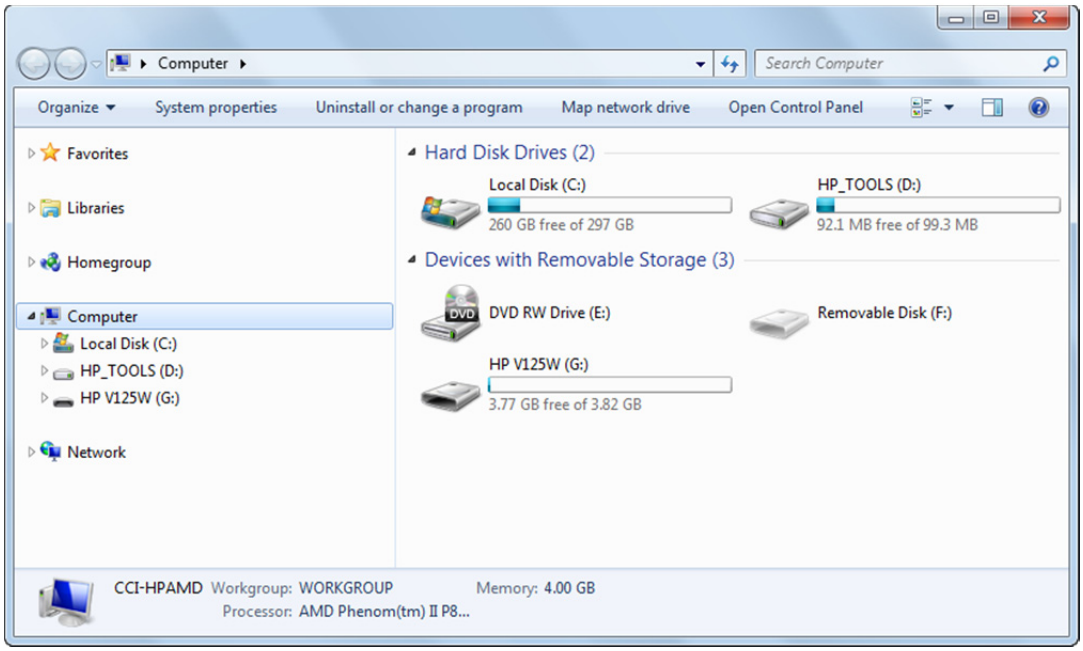
If hidden shares is still not working, you should check that the Windows Firewall is opened for sharing:

1. Open the Control Panel and select **System and Security**.
2. Click **Windows Firewall**.
3. Click **Allow a program or feature through Windows Firewall**.
4. Scroll down the list of Allowed programs and features, and ensure that the File and Printer Sharing check box is turned on for **Home/Work**.

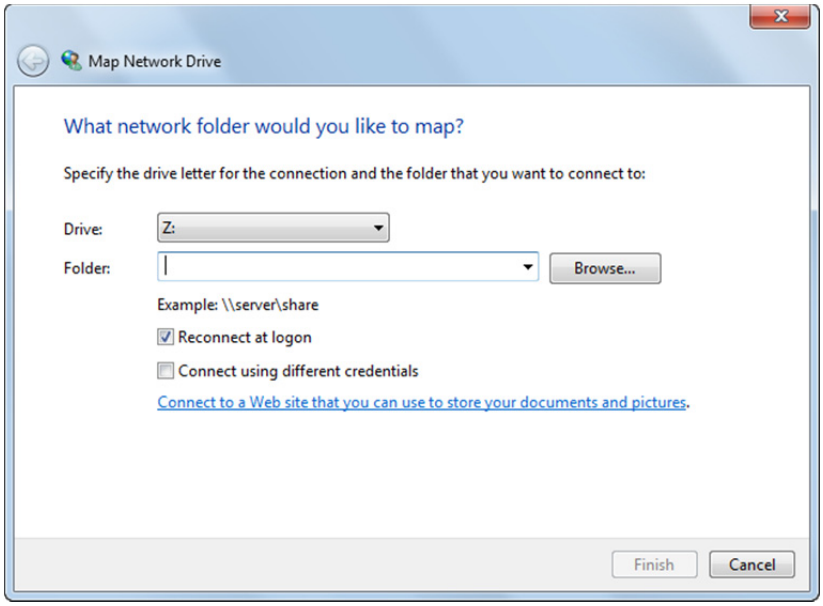
# Mapping Drives

Once you have created shares, you may find it convenient to map drives to the shares to provide easy access. When you map a drive, you create a shortcut to a network location and that shortcut is represented by a drive letter. Mapped drives appear in Windows Explorer as if they were local drives.

The following steps illustrate how to map a network drive. Open Windows Explorer, then click **Computer**.




In the toolbar, click **Map network drive** to open the Map Network Drive dialog box.

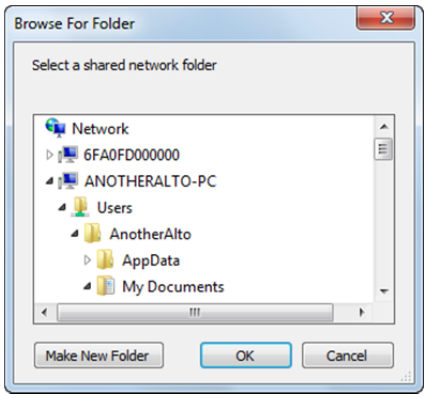



Windows suggests a drive letter you can assign to the map. Select any available letter in the drop-down list, then in the Folder box, type the path of the folder or computer.

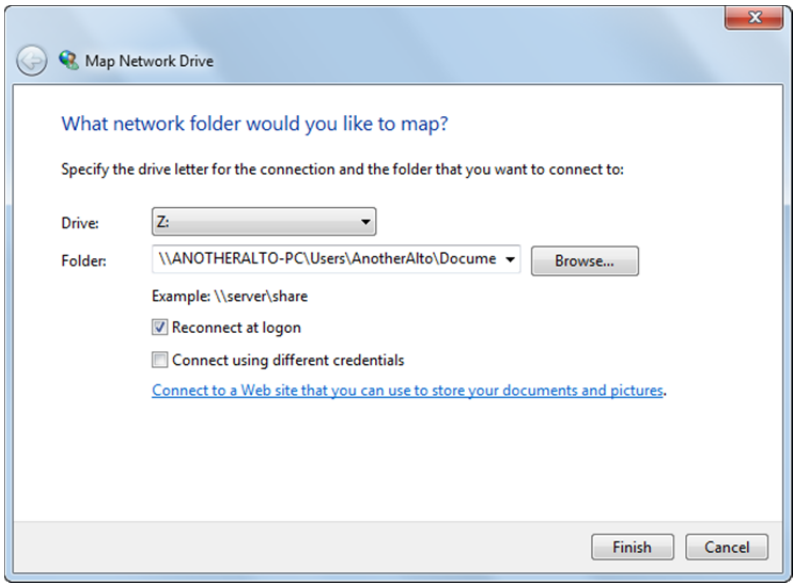
You can type a path using the Universal Naming Convention (UNC). A UNC consists of a computer name and a share name. For example, to refer to a share named "ShareMe" in the My Documents folder on a computer named AnotherAlto-PC, the UNC would be:

\\ANOTHERALTO-PC\Users\AnotherAlto\Documents\ShareMe.

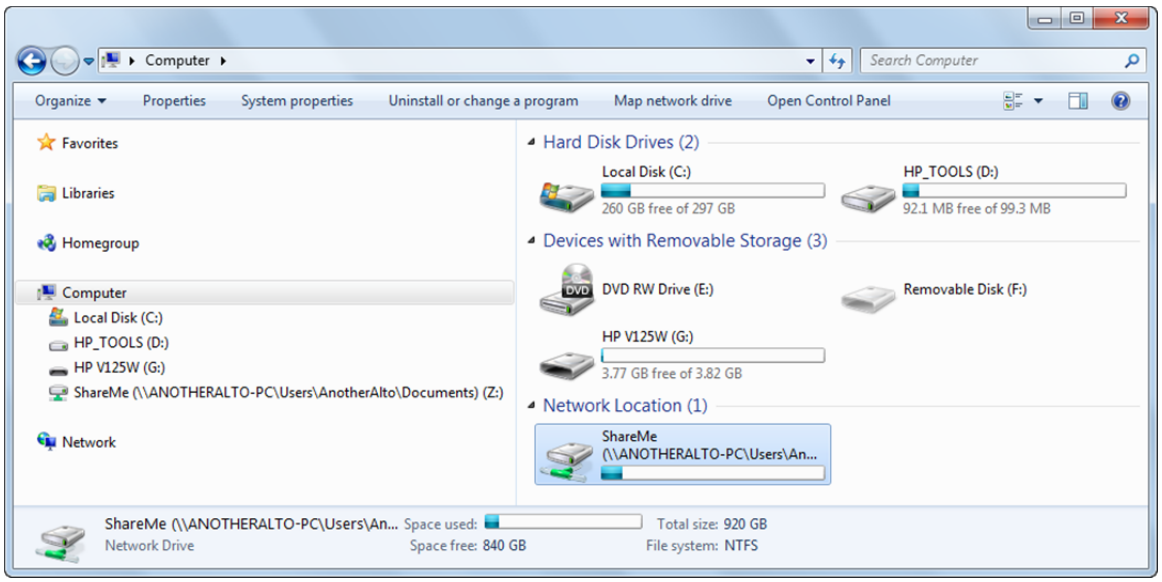
You can also click the **Browse** button to navigate to the folder or computer to see the shared folders available to you.




When you navigate to the share folder, select it, then click **OK** to add the path to the Folder box.




To connect every time you log on to your computer, select the **Reconnect at logon** check box. Click **Finish** to complete the process. The mapped network drive now appears in Windows Explorer as if it were a local drive.




To "unmap" or disconnect a (share) drive, right-click the share in the navigation pane, then select **Disconnect**.

## Mapping a Drive at the Command Prompt

You can also map a network drive at the command prompt with the **net use** command. The command syntax is: **net use x: \\computer name\share name,** where *x:* is the drive letter you want to assign to the shared resource. To map the share described above to the drive letter w, for example, the command would be:

```
net use w: \\ANOTHERALTO-PC\Users\AnotherAlto\Documents\ShareMe
```

To unmap the share, use the disconnect command. The syntax is: **net use x: /delete**, where x: is the drive letter of the shared resource. To unmap the share described above from the drive letter w, the command would be:

```
net use w: /delete
```

System administrators frequently use the net use command to automate tasks; for example, setting up a group policy or mapping a drive on a large number of computers.

# Understanding Permissions

Permissions are rules associated with objects on a computer or network, such as files and folders. Permissions determine whether you can access an object and what you can do with it when you access it. For example, you might have access to a document on a shared folder on a network. And even though you can read the document, you might not have permissions to make changes to it.

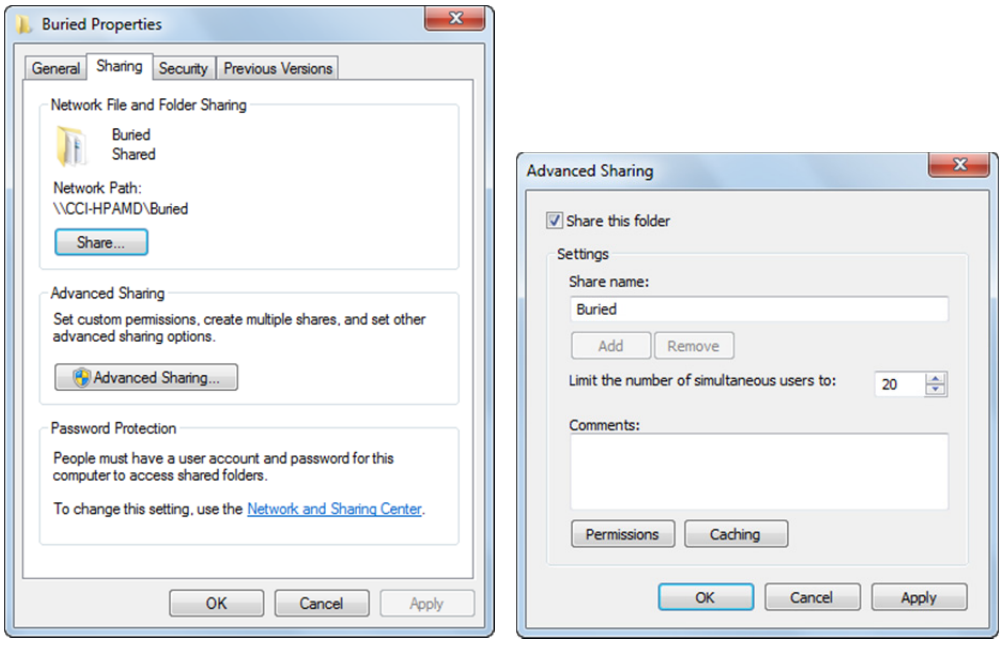
There are two types of permissions that control the types of actions users can perform on network resources. These two types of permissions are: share permissions and NTFS file system permissions.

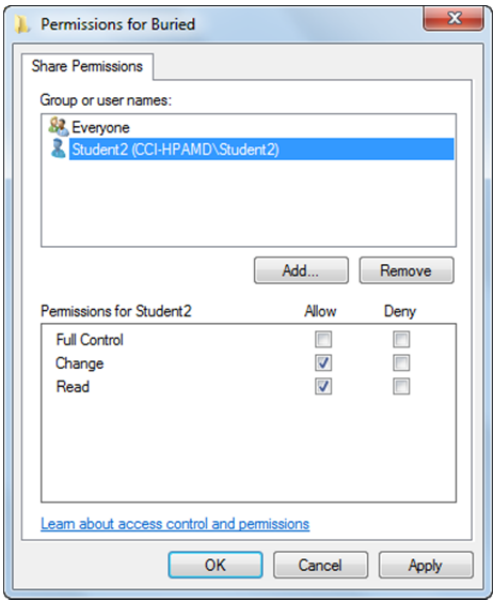
## Share Permissions

Share permissions are used to control who can access shared folders, and to control the actions users can perform when they access those folders from a remote computer over the network. There are three share permissions:

| | |
|---|---|
| **Read** | User can view the names of files and folders within the share, view the contents of files, and execute application program files. |
| **Change** | Users can view the names and contents of files and folders, and can create new files and folders, modify the contents of files, and delete files and folders. |
| **Full Control** | Users can perform all the actions allowed by the Change permission, and they can manage permissions on the share. |

Share permissions are set on the Sharing tab of the Properties dialog box, by clicking **Advanced Sharing**, and then clicking the **Permissions** button (see Advanced Shares topic above).






By default, all remote users (using the Everyone group) have read access to a shared file or folder.

## NTFS Permissions

If the volume is formatted as FAT16 or FAT32, you do not have the ability to set file system permissions. Therefore anyone who logs onto that computer can view or change any of the files or folders in that volume. If the volume is formatted as NTFS, you can protect files and folders by defining how they can be accessed and by whom. NTFS permissions also offer more options for control access than share permissions; this will give you a greater degree of control over what users can do with files and folders.

NTFS permissions may be:

| | |
|---|---|
| **Explicit** | An explicit permission is one that is set on an individual folder or file. |
| **Inherited** | An inherited permission is one that is passed on from a parent folder to the files or subfolders stored within it. By default, a file inherits the permissions of the folder in which it was created. Subfolders also inherit the permissions of their parent folders. |

Large enterprises will typically have a very large number of files and folders stored on many servers, as well as many users who want access to them. Therefore, you should always try to keep permissions simple and easy to manage by following two guidelines:

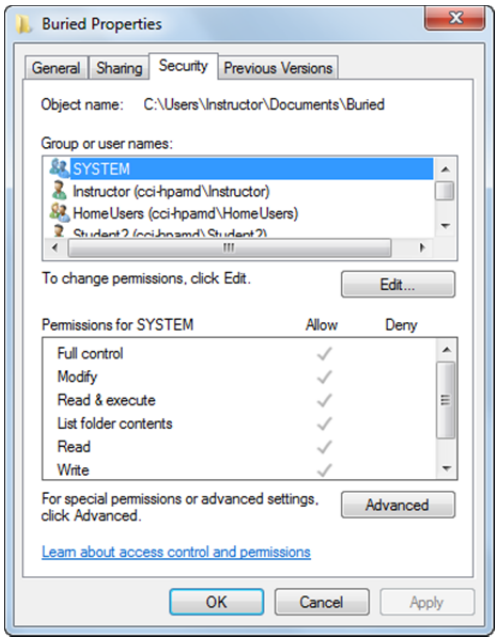
- Assign permissions to groups of users who have similar needs instead of individual users.
- Set the explicit permissions as high as possible in the folder hierarchy (i.e. closer to the root directory) of a volume. Use inherited permissions for as many subfolders underneath as possible.

The standard NTFS file and folder permissions are described in the following table. Note that not all permissions apply to all objects:

| Permission level | Description |
|---|---|
| **Read** | Users can see the contents of a folder and open files and folders. |
| **Write** | Users can see the contents of a folder, open files and folders, create new files and folders and make changes to existing files and folders. |
| **Read and execute** | Users can see the contents of a folder, open files and folders and run programs in a folder. |
| **List folder contents** | Users can view contents of folders and run program files, but not read the contents of the files contained within the folders. This permission can only be applied to folders. |
| **Modify** | Users can see the contents of a folder, open files and folders, create new files and folders, make changes to existing files and folders, run programs in a folder, and delete files and folders. |

| | |
|---|---|
| **Full control** | Users can see the contents of a folder, open files and folders, create new files and folders, make changes to existing files and folders, run programs in a folder, delete files and folders, and manage permissions on the folder and the files and folders contained within it. With full control, a user can take ownership of the folder. Full control is a very powerful permission. |
| **Special Permissions** | Also referred to as advanced permissions. This feature gives administrators more precise control over exactly the kind of access to grant to users and groups. |

NTFS permissions are set on the Security tab of the Properties dialog box.




*Explicit denial of a permission overrides the granting of that permission through any other group membership or user account.*

You can also specify that a permission type be explicitly denied.

Under the NTFS file system, every object has an owner. In most cases, the person who created the file or folder is the owner. However, if the system created the object, then the owner is the Administrators group. To change NTFS security permissions, you must be the owner of the file or folder or have permission granted to you by the owner to change that object's security settings. However, any member of the Administrators group automatically has the ability to Take Ownership of any file or folder on the system. In addition, groups or users who have been granted Full Control on a folder can delete files and folders within that folder regardless of the permissions protecting those files and folders.

## Combining Share and NTFS Permissions Together

It is important to understand that share permissions and NTFS permissions are not the same. They define user access privileges on two different levels.

### Most Restrictive for Both Types

Share permissions apply only when you try to access files or folders located on a remote computer using the network; they do not apply if you log directly onto that computer. When you do access resources over the network, the two permissions work together in the mos t restrictive way. The network share permissions will kick in first, rejecting anyone who does not have any access rights or allowing them to enter with the specified share permissions. The NTFS permissions are then applied, and some or all permissions may be removed. NTFS permissions will never add greater permissions to what was allowed by share permissions.

For example, if a share provides Read permission, and a folder within the share provides NTFS Modify permissions, the user will still have only Read permissions when accessing the resource through the share. In this case, the share permissions are limiting what the user can do.

At the same time, the NTFS permissions apply whether you access resources locally or through the network. For example, if you have Change permission via the network share, but your NTFS only allows Read then you will only have Read access. This is to ensure that users do not try to circumvent the access rights by going through the network instead of accessing the files while logged onto the computer directly.

### Understanding Effective Permissions

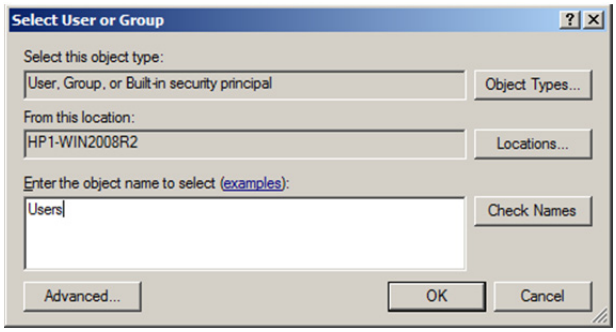
When determining effective permissions, it is important to understand how group membership can change permissions. Your user account on a system defines you as a user on that system, or in the Windows domain to which the system belongs. System administrators often assign particular users membership in one or more groups. Often, a user belongs to several groups.

Permissions are cumulative; that is, user accounts will receive the permissions granted to the local system, as well as any groups to which they belong.

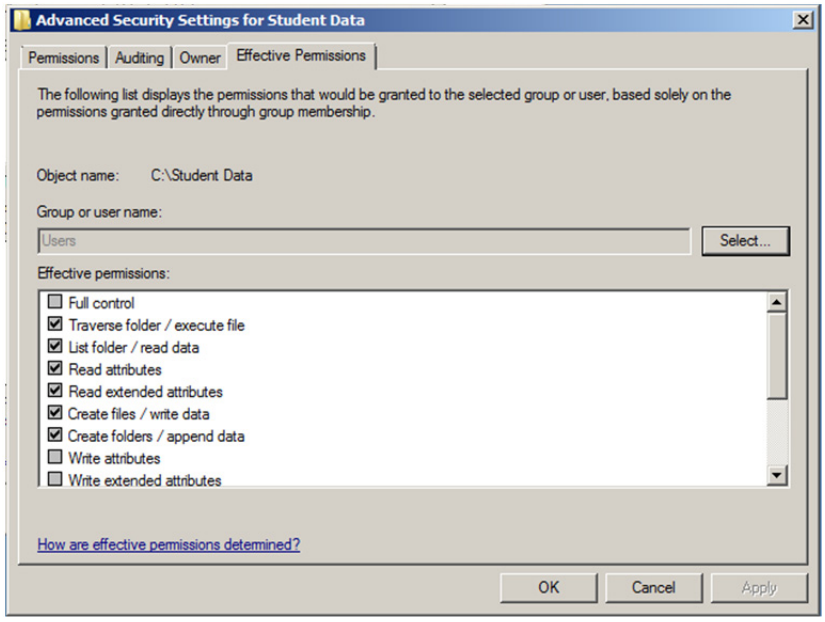
For example, if user Bob has NTFS Read permissions on a folder (granted specifically to his user account), and also has Modify permissions on the same folder (granted through a group of which Bob is a member), then Bob will have Modify permissions when accessing the folder.

To help you, Microsoft provides a tool that will display the NTFS permissions in effect on a file or folder for any local or domain group or individual user account. For example, you can display Bob's permissions to a folder by following these steps:

1. In Windows Explorer, navigate to the folder where the file or folder is located.
2. Right-click on the file or folder and click **Properties**.
3. Click the **Security** tab, and click **Advanced**.
4. In the Advanced Security Settings dialog box, click the **Effective Permissions** tab.
5. Click **Select** to display the Select User, Computer, or Group dialog box.
6. Enter the user account name or group and click **OK**.




The Effective Permissions tab now displays the permissions that apply for the selected user or group:



Note that this tool will calculate the effective permissions that apply only to the file system. It does not factor in share permissions that may reduce the access privileges.

# Sharing Printers

If you have a printer attached to your computer, you can share it with anyone on the same network. It doesn't matter what type of printer you have, as long as it's installed on your computer and is directly attached with a USB cable or other type of printer cable.

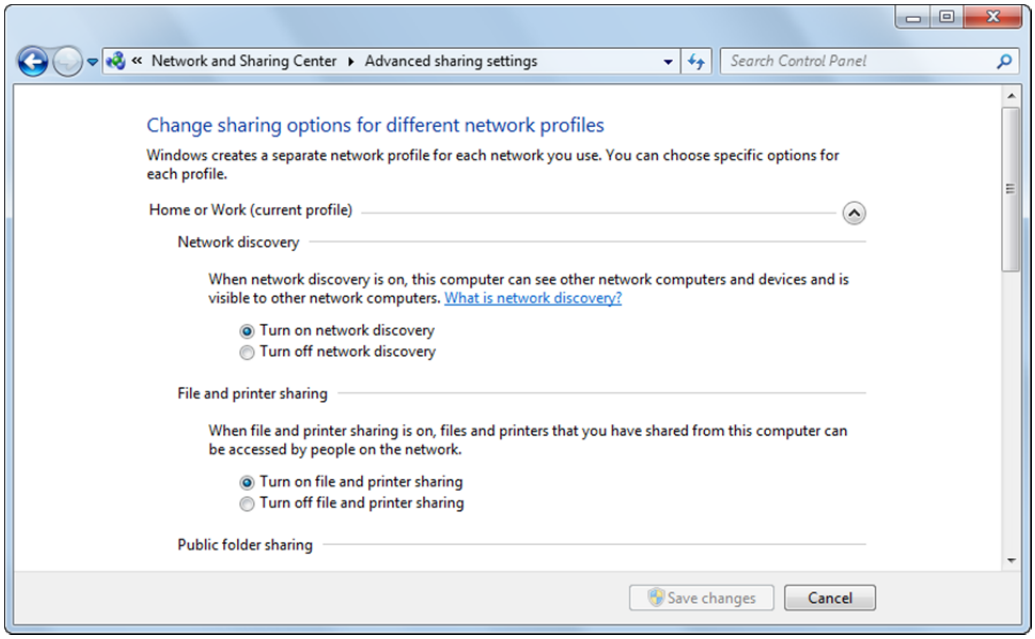
A shared printer is one that is directly connected to a computer on the network. When users access a shared printer, they access that printer through the computer to which it is connected. For this reason, if the computer that is sharing the printer is sleeping or turned off, the printer will be unavailable. A shared printer is not the same as a network printer.

A network printer is one that is connected directly to a network device such as a switch or router. Users on the network can connect to a network printer directly, without having to go through an intermediate network node. (You will learn about network printers in Lesson 5.)

## Creating Printer Shares

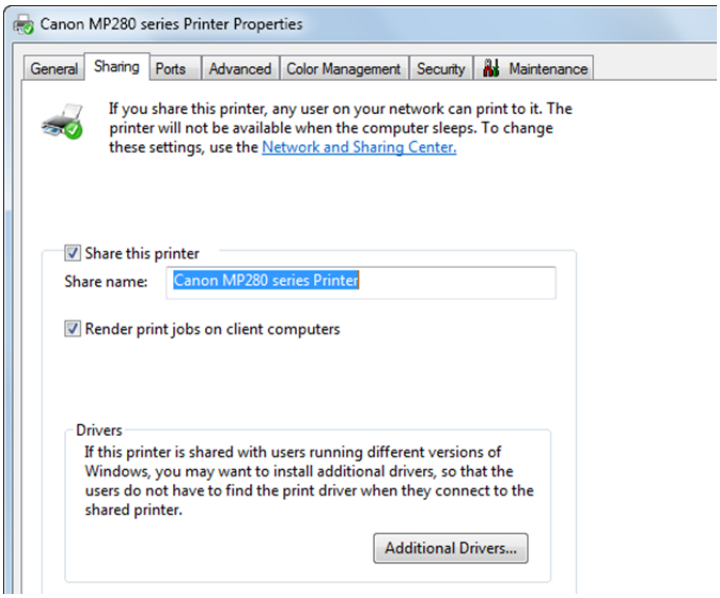
To share a printer that is installed and configured on your computer:

1. Ensure that file and printer sharing is turned on. This setting can be found on the Advanced Sharing page in the Control Panel. Open the Control Panel, open the Network and Sharing Center, then click the **Change advanced sharing settings** link. Select **Turn on file and printer sharing** if necessary, then click **Save Changes**.




Share the printer in the Devices and Printers page of the Control Panel.

2. Open the Devices and Printers page of the Control Panel, right-click the printer you want to share, then select **Printer properties** to open the Printer Properties dialog box. Click the **Sharing** tab. Select the **Share this printer** check box and either accept the suggested share name or specify a new share name. Select the **Render print jobs on client computers** option to alleviate some of the processing overhead for the local computer (this option is selected by default), then click **OK**.

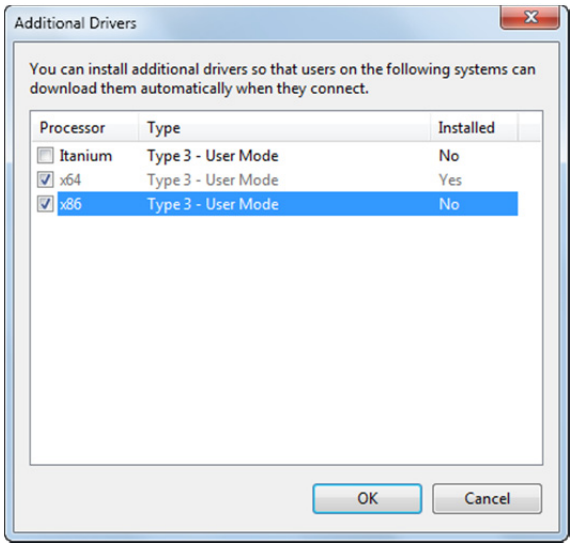



## Providing Printer Drivers

If you are sharing your printer with computers running different versions of Windows, you can provide the printer drivers that these systems need to use to print on your printer. (A printer driver is a program that enables a printer to communicate with the operating system.) For example, if you are running a 64-bit version of Windows 7 and another computer on your network is running a 32-bit version of Windows, that system will need 32-bit printer drivers.

When you provide the drivers, a system running the 32-bit operating system will automatically download and install the drivers when it first attempts to connect to the printer. In order to make these drivers available you must install them. You will need access to the CD or other media that contains the drivers that shipped with the printer. You may also download additional drivers from the manufacturer's Web site.

To install the additional drivers, click the **Additional Drivers** button on the Sharing tab of the Printer Properties box to open the Additional Drivers dialog box. You can specify to install drivers for Itanium systems, 64-bit systems and 32-bit system. Select the drivers you want to install, then click **OK**.

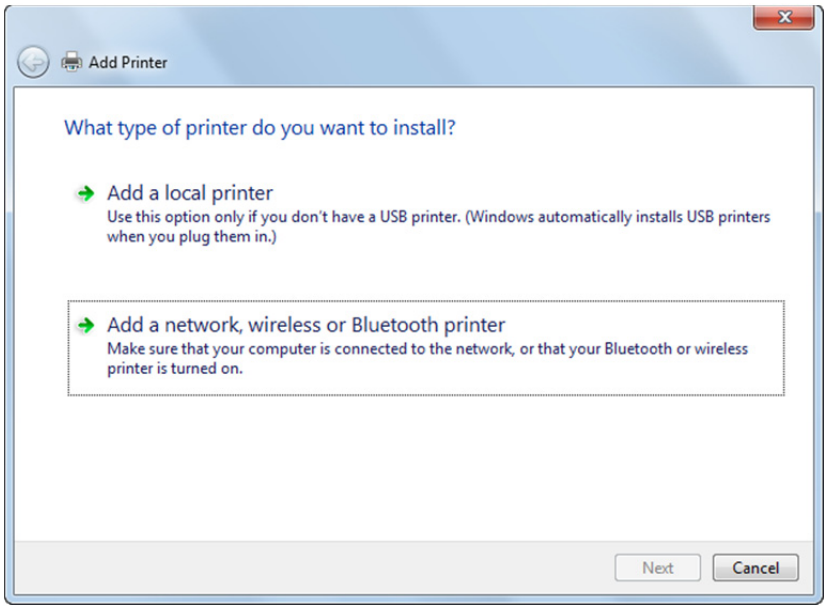



If you do not provide the printer drivers, other users will have to find and install them before they can use your shared printer.

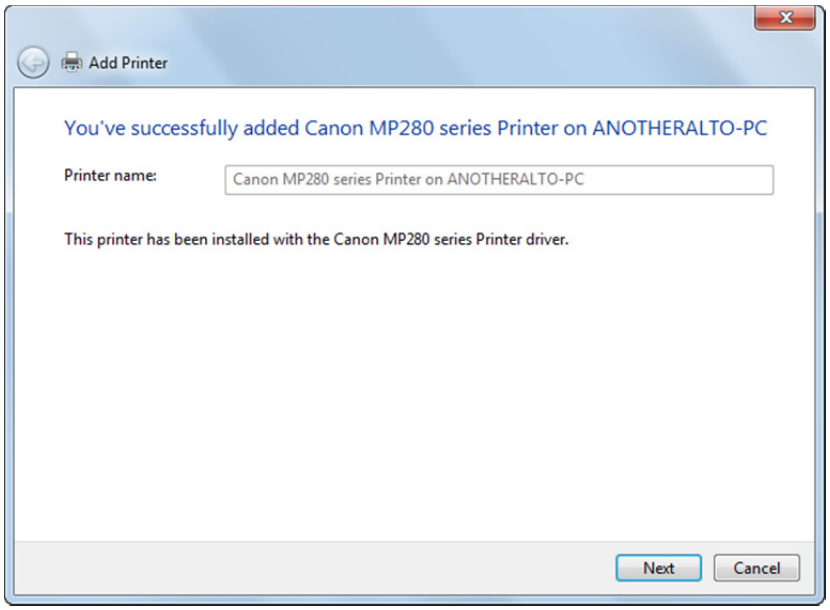
## Connecting to a Printer Share

Users must connect to a printer share in order to use a shared printer. To connect to a printer share:

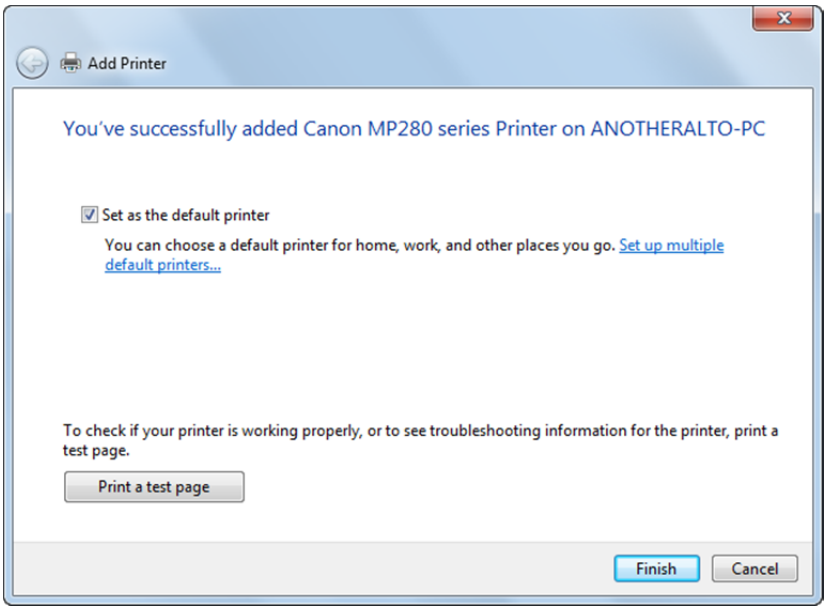
1. Open the Devices and Printers page in the Control Panel, then click the **Add a printer** button to open the Add Printer dialog box. Click **Add a network, wireless or Bluetooth printer**.




2. Select the printer to which you want to connect, then click **Next**. Windows displays a message when it successfully connects to the printer.

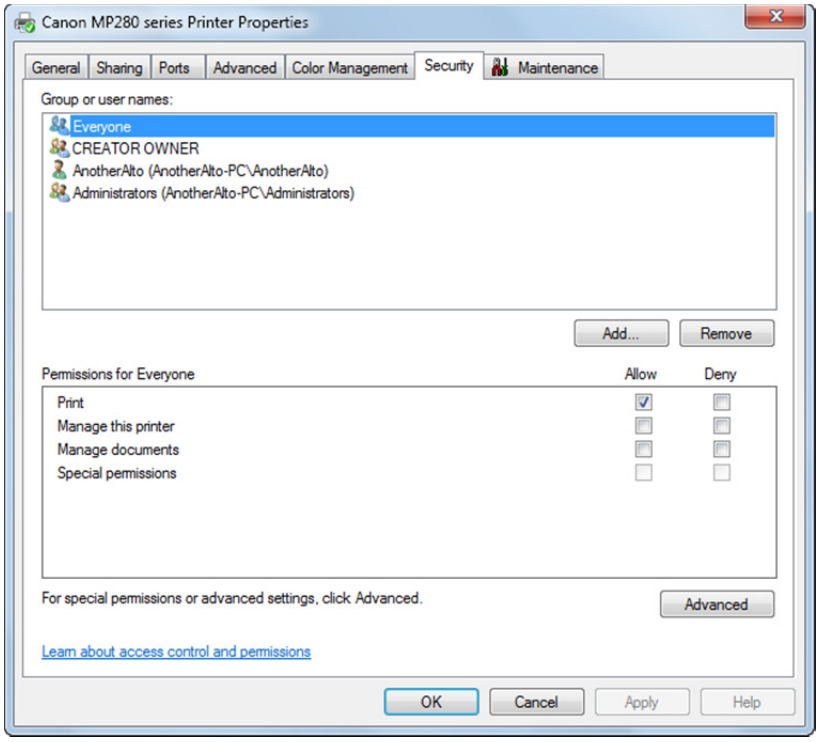



3. Click **Next** and you can specify whether you want to make the shared printer your default printer. You can also print a test page. When you are done, click **Finish**.




## Managing Printer Shares

You can control what other users are allowed to do while accessing your shared printer by managing the printer share. To manage a printer share, open the Security tab of the Printer Properties dialog box.




You can specify the following permissions for each user or group:

| | |
|---|---|
| **Print** | The user can print. |
| **Manage this printer** | The user can rename, delete, share, choose preferences and manage printer permissions. |
| **Manage documents** | The user can manage print jobs, pause and restart print jobs, or delete print jobs. |
| **Special permissions** | The user can change ownership of the printer. |

# Understanding Encryption

Objective 4.3 5.2

*Encryption* is the process of converting data into an unreadable form of text. Decryption is the process of converting the encrypted data back to its original form. Encryption and decryption are performed through keys. A key is a mathematical algorithm. The more complex the encryption algorithm, the harder it is to decipher the encrypted message without access to the key. Encrypted data is referred to as ciphertext; unencrypted data is referred to as plaintext.

Encrypted text cannot be read without the correct decryption *key* to decrypt, or decipher, the encrypted data back into plaintext. Because encrypted text is unreadable by anyone who does not possess the correct key, data encryption helps secure sensitive data stored on hard drives or network shares.

Encryption can be applied to data at rest, such as data stored on computer hard drives or removable USB flash drives, or to transmitted data such as email, Internet traffic, wireless networks, and cell phone calls. In all of these applications, the intent is to prevent others from seeing the contents of the data, and to protect the integrity of the data by preventing data from being lost and extra data from being inserted.

## Encryption Concepts

There are three encryption models. These are: symmetric-key, asymmetric-key and hash.

### Symmetric-key (Single-key) Encryption

In *symmetric-key*, or single-key, encryption, one key is used to encrypt and decrypt messages. With this method of encryption, all parties must know and trust one another completely, and have confidential copies of the key. An example of a symmetric key is a simple password you use to access an automated teller machine, or to sign in to your ISP.

Symmetric encryption is fast, allowing you to encrypt a large amount of information in less than a second.

### Asymmetric-key (Public-key) Encryption

*Asymmetric-key encryption* uses two keys, a public key and a private key. The public key is known to all sending and receiving parties involved, and the private key is used by the recipient to decrypt the message. In fact, the public key can be openly published for anyone to see and use. However, the recipient must keep the private key a secret. The public and private keys are mathematically related so only the public key can be used to encrypt messages, and only the corresponding private key can be used to decrypt them. Together, these keys are known as a key pair.

A drawback of asymmetric-key encryption is that it is slow, due to the complex mathematical calculations that the algorithm requires. Many applications use asymmetric-key encryption to encrypt only the symmetric key that encrypts the body of the message.

### Hash (One-way) Encryption

*Hash encryption* (also called one-way encryption) is an encryption method in which hashes are used to verify the integrity of transmitted messages. A *hash* (also called a message digest) is a number generated by an algorithm from a string of text. The generated hash value is smaller than the text itself, and is generated so it is nearly impossible for the same hash value to be generated from some other text. The hash is as unique to the text string as fingerprints are to an individual.

Hash algorithms are generally used to verify the validity of digital signatures, which authenticate message senders and recipients. Hash functions are also used in automatic teller machines. When a user swipes a card, and enters a personal identification number (PIN), the machine calculates the hash on the PIN that the customer enters, then compares it to the hash code stored in the magnetic stripe on the back of the card. Using this method, the PIN is secure, even from the automated teller machine and the individuals who maintain it.

## Encrypting File System (EFS)

In Windows 7, you can use Encrypting File System (EFS) to encrypt individual files and folders. EFS can be used only on files and folders residing on NTFS volumes. You cannot use EFS to encrypt files on a FAT32 volume.

EFS works by generating an encryption key called the file encryption key (FEK) and then encrypting the data with that key. The FEK itself is then encrypted with the user's public key and stored with the data. The public key is provided in a file encryption certificate that is either automatically generated by the system, or generated by the network administrator. The file encryption certificate is a digitally signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key.

In EFS, symmetric encryption is used to encrypt the actual data, and then asymmetric encryption is used to encrypt the FEK. When the user accesses the encrypted data, the FEK is decrypted with user's private key, then the FEK is used to decrypt the data.

Encryption and decryption occur automatically as long as the user who initially encrypted the data is logged on to the machine.

## Encrypting Files and Folders

You use EFS by turning on the encrypted attribute in Windows Explorer. To encrypt a file:

1. Navigate to the file in Windows Explorer
2. Right-click the file and select **Properties**
3. On the General tab, click the **Advanced** button
4. Check the **Encrypt contents to secure data** check box, then click **OK**

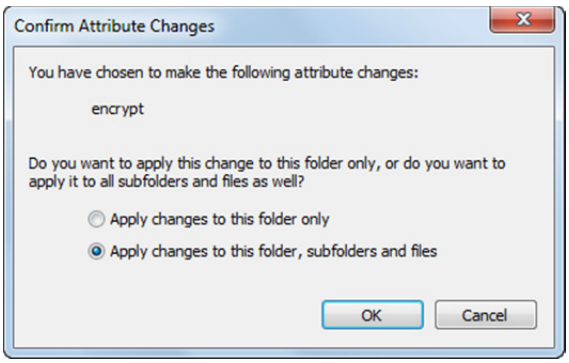
   Windows 7 displays the following warning box when you specify to encrypt an individual file:


Some programs create a temporary copy of a file while a user is editing it. The temporary file remains open until all changes are saved to disk and the file is closed. Windows 7 sees this as a security issue because the temporary file will not be encrypted if its parent folder is not encrypted. Windows 7 offers you the option of encrypting the parent folder as well.

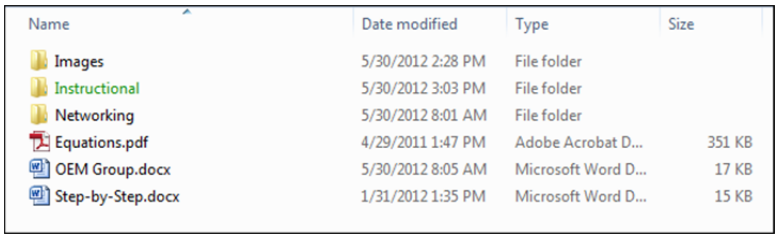
To encrypt a folder:

1. Navigate to the folder in Windows Explorer
2. Right-click the folder and select **Properties**
3. On the General tab, click the **Advanced** button
4. Check the **Encrypt contents to secure data** check box, then click **OK**

When you encrypt a folder, you are given the option to apply changes to the folder only, or to the folder and its subfolders and files.




When you encrypt a file or folder, it displays in green in Windows Explorer.

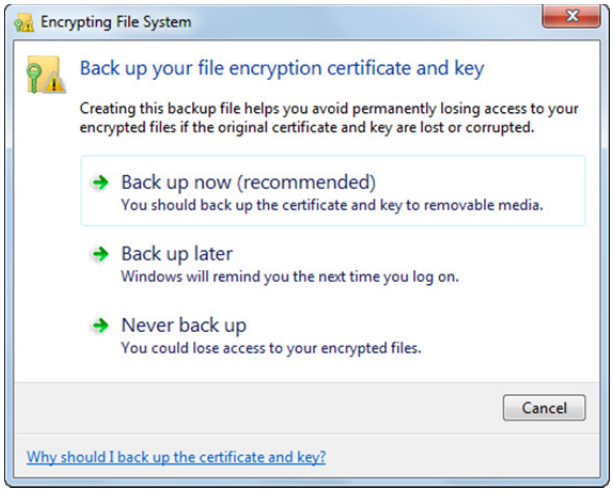


| Name | Date modified | Type | Size |
|---|---|---|---|
| Images | 5/30/2012 2:28 PM | File folder | |
| Instructional | 5/30/2012 3:03 PM | File folder | |
| Networking | 5/30/2012 8:01 AM | File folder | |
| Equations.pdf | 4/29/2011 1:47 PM | Adobe Acrobat D... | 351 KB |
| OEM Group.docx | 5/30/2012 8:05 AM | Microsoft Word D... | 17 KB |
| Step-by-Step.docx | 1/31/2012 1:35 PM | Microsoft Word D... | 15 KB |

## Backing Up Certificates and Keys

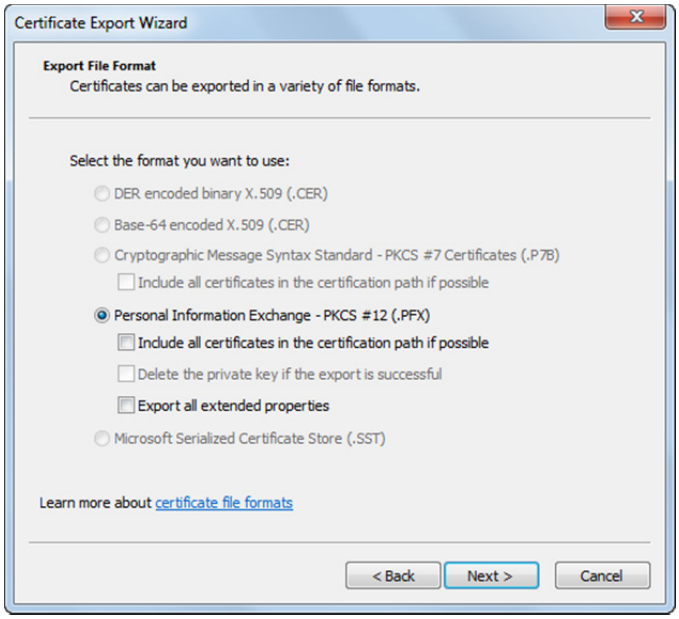
The first time you use EFS on a system, a balloon appears in the notification area advising you to back up your encryption keys. You can export a copy of the file encryption certificate and the FEK to removable media. It is important to have a backup copy, in case the certificate and key stored on the system becomes lost or corrupted.


Click the balloon to view options for backing up your file encryption certificate and key.

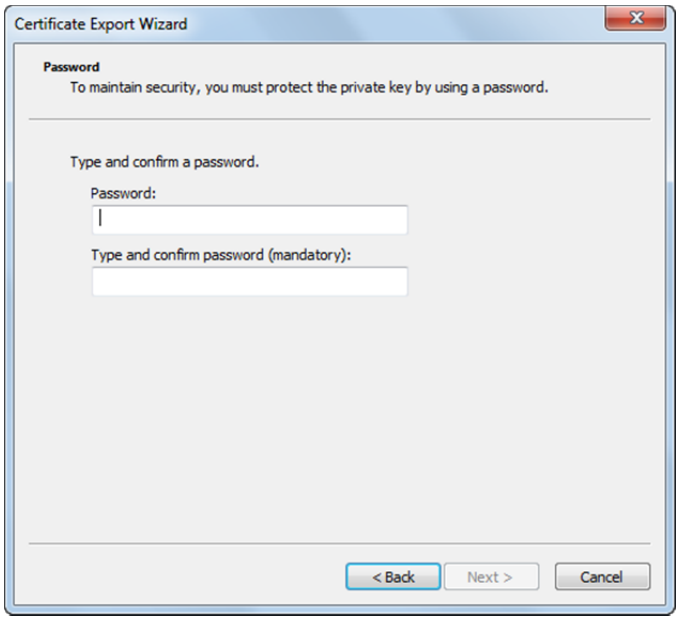



Select **Back up now (recommended)** to open the Certificate Export Wizard.

Click **Next**.




Certificates can be exported in a variety of file formats. The default file format – Personal Information Exchange - PKCS #12 (.PFX) – is suitable for exporting a key to a USB flash drive. After you select a file format and click **Next**, you are asked to enter and confirm a password.




After you enter and confirm a password and click **Next**, you are asked to supply a file name and location for the exported file. You can browse to a location or type the path and file name. Once you click **Next**, the certificate and key are exported. Click **Finish** to close the wizard, and click **OK** to close the message box that tells you the export was successful.

If your certificate and key embedded in the system becomes lost or corrupted, you can double-click the exported file to launch the Certificate Import Wizard, which imports the certificate and key back onto the system.

# BitLocker

While you can use EFS to encrypt file or folders, you can use BitLocker on Windows 7 Ultimate/Enterprise systems to encrypt entire volumes. You can use it to encrypt:

- Volumes that contain an operating system – to encrypt an OS volume, a separate volume of approximately 100 MB must exist to provide access to files needed at boot time. These files are accessed before the OS volume has been decrypted. This 100 MB volume is created automatically when Windows 7 is installed.
- Storage-only volumes (hard disks or partitions that do not contain an operating system) – to encrypt a storage-only volume, the system must include a Trusted Platform Module (TPM) chip for storage of encryption keys or a USB flash drive for storage of encryption keys.
- USB flash drives – to encrypt a USB flash drive, you can use BitLocker To Go.

You can access BitLocker and BitLocker To Go through the Control Panel and following the prompts presented in the wizard. You will be asked for either a password or a smartcard to use as the unlock mechanism for the drive. You will also be prompted to save recovery information so that you can restore the drive and access the encrypted data.

If you are using BitLocker on an internal drive, you are also given the option to automatically unlock the drive so that a password is not required each time you boot up.

# Managing Encryption Keys

As you have already learned, encryption keys are generated and managed using digital certificates. You can export your encryption certificate and key for safe keeping in case the one stored on the system becomes lost or damaged. However, in an enterprise consisting of hundreds or thousands of users, certificates and keys are managed centrally. This type of management requires the use of public key infrastructure (PKI) to manage the certificates.

## Digital Certificates and Public Key Infrastructure (PKI)

A digital certificate is a small file that proves the identity of a person, a system or a process. Digital certificates are widely used for secure transactions over the Internet. They help minimize security risks by authenticating users and systems.

A trusted third party, called a certificate authority (CA), is responsible for verifying the legitimacy of the digital certificate. After you receive a legitimate digital certificate from a person or system, you can be reasonably sure you are communicating with the proper party.

A certificate must be digitally signed by a certificate authority to be valid. A digital signature is a unique identifier that authenticates a message, as would a standard, written signature. It is the combination of a private key generated by an asymmetric-key algorithm and hash encryption.

Digital certificates include the following data about the certificate owner:

- Name, company and address
- Public key
- Certificate serial number
- Dates that the certificate is valid
- Digital signature of the certifying company

SSL (Secure Socket Layer) is a protocol designed to enable data to be transmitted securely between two computer systems through a network connection. SSL is now evolved to the Transport Layer Security (TLS) protocol used for secure communications over the Internet. SSL is still used for secure communications in other non-Internet traffic.

When a client system wants to establish a secure communication with a server, both systems must follow an elaborate process called a handshake. Every network communication between two systems involves a handshake, but a secure connection also requires an exchange of encryption keys. The certificate plays a key role by supplying the server's public key to any client system that wishes to communicate to it.

1. The client system initiates contact by sending a SSL greeting message to the server. The client is doing the equivalent of saying "Hello, are you there?" This greeting message includes a list of the encryption algorithms and compression methods that the client is able to understand.
2. The server will respond with a greeting message or an error message. The server is doing the equivalent of saying "Hello" or "I am not available right now, call again later." This response includes the encryption algorithm and compression method that the server has selected from the list that the client provided.

3. If the server responded with a greeting, it will also send one or more certificates to the client. This is like saying “My name is …..” because it is presenting its identity card back to the client.
4. Depending on the encryption scheme, the server may ask the client for its digital certificate. This is like the server asking “And who are you?”
5. The client inspects the certificate(s) sent by the server and validates the information. If a problem is found, a message is displayed on the screen to warn the user that the server could not be authenticated (“This identity card is fraudulent!”).
6. If the server’s certificate is valid, then the client system creates a secret key, encrypts it using the server’s public encryption key from the certificate, and sends it to the server.

The secret key must be encrypted because anyone who gets a hold of it will be able to listen in on the conversation and decrypt everything. The purpose of the server’s public key is to keep the client's secret key secret. Only the server that sent the public key has the private key to decrypt any messages that have been encrypted using the public key. Not even the client system can decrypt the message that it just created using the server's public key because it is a one-way encryption (hence the term asymmetric) scheme.

7. If the server asked for a certificate, the client will also send it to the server.
8. If the client responds with “No certificate” or the client’s certificate cannot be validated, the server will most likely stop responding. Otherwise, the server will decrypt the client’s secret key using its private key.
9. Both the client and server use the secret key to create the session key.

This session key is the symmetric key that both the client and server will use to encrypt and decrypt all future messages to each other.

10. The client and server both switch to encryption mode and the user is now able to use the secure website in privacy.

Although there have been numerous attempts (some were successful) to crack parts of this encryption scheme, this communication process has many layers to ensure that it is a practical and secure method of exchanging data between two systems.

The procedures described above and the rules that your web browser and websites must follow to establish the secure communication are all part of the Public Key Infrastructure designed to ensure you can trust the communication; that is, ensuring the other party is who they claim they are, no one else is spying on your communication, and no one else can modify any part of the communication being exchanged. This is a critical component for enabling business to consumer (B2C), business to business (B2B), and business to government (B2G) transactions. In addition to authenticating the identity of the entity owning a key pair, PKI also provides the ability to revoke a key if it is no longer valid. A key becomes invalid if, for example, a private key is cracked or made public.

SSL certificates can also be used internally within an enterprise or over the Internet for non-public communications. For example, an enterprise may restrict web service access to a server (for example, a server containing confidential employee salary information) by requiring the client system (which may be another server) to present a SSL certificate when it wants to communicate with the server. In these applications, certificates are used to replace the need for a logon ID and password. As a result, a regular payroll run can occur and data transmitted between servers (e.g. sending direct deposit information to banks) without any person having to log on to a computer, thereby improving the overall security of the data and the payroll processing system. To maintain good security, system administrators will need to ensure the certificates are added only to computers that require them.

Similarly, doctors and pharmacists exchange patient medical data with government and private health providers using SSL certificates. The health organization will issue a unique digital certificate to each healthcare professional, who adds it to their computer system. Medical data can then be exchanged between these servers in realtime instead of requiring a person to press an “Update now” button. The health organization can identify who the user is by their SSL certificate, and control their access privileges accordingly. The SSL certificates are created, managed, and terminated by the health organization. However, the certificate will identify only the user’s computer system that is connected. Each individual user (e.g. doctor) in the healthcare practitioner’s office must still log on with their personal ID and password when they need to enter data or run inquiries from their client system.

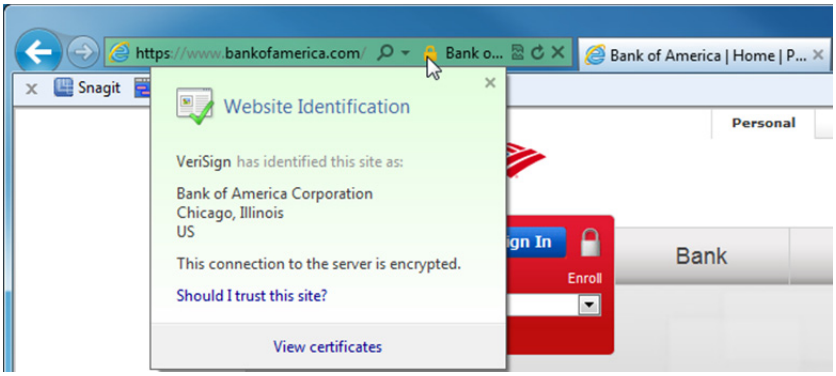
# Exercise 4-2: Displaying a Digital Certificate for a Website

In this exercise, you will examine the digital certificate for a secure website.

1. Start Internet Explorer, and enter: `bankofamerica.com` into the address bar. Alternatively, you can enter the URL for another secure website of your choosing.

Notice that you are automatically redirected to another website where the URL is preceded by the prefix "https://" and a padlock icon is displayed in the address bar. The presence of these two indicators will confirm that you are viewing a secure website. In general, if you do not see both of these indicators, you should close the web page immediately because you do not have a secure connection with your intended website.

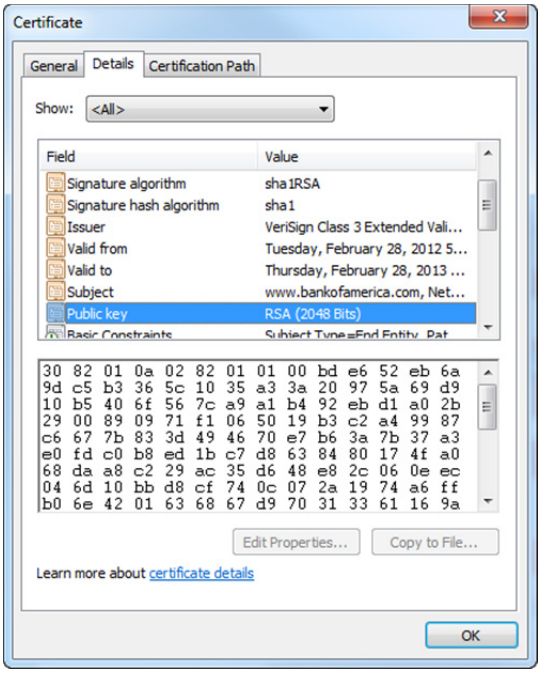
2. Click on the padlock icon in the address bar.




A pop-up box is displayed. It displays the name of the third party certificate authority (VeriSign in this example), and allows you to examine the SSL certificate that has been issued by the Bank of America Corporation. VeriSign uses its reputation to confirm that this SSL certificate is genuine.

If the address bar is green, this indicates that the website is using an extended validation certificate, an enhanced version of a SSL certificate.

3. Click **View certificates** at the bottom of the pop-up box.
4. In the Certificate window, scan through the contents of the General tab to view the certificate information.
5. Click on the **Details** tab, then scroll down and click on **Public key** to display it



This screen example shows a public key that is 2,048 bits long, and displayed as 256 groups of two hexadecimal digits (each hex digit is 4 bits long). This public key is used to encrypt data to be sent to the Bank of America, but can't be used to decrypt data; only the Bank of America has a corresponding private key that is able to perform the decryption, hence the term asymmetric keys. However, asymmetric key encryption allows only one way communication. Your system then uses the public key to encrypt one or more symmetric keys (called session keys) that are used for two-way communications between your system and Bank of America. Because a symmetric key is used for both encrypting and decrypting data, both parties can exchange data but anyone trying to intercept and read the data will see only a string of apparently random characters. The Bank of America will use their private key to decrypt your message containing the symmetric keys and will then begin encrypting all future communications with your system using these keys. When you complete your business transaction with the Bank of America – or you do not send another secure message to them within a period of time (your session is "timed out") – your session keys become invalidated and any further communication with the Bank of America website will create a new set of session keys (and any memory of your previous session is lost).

6. Click **OK** to close the Certificate window.

In this exercise, you examined the digital certificate for a secure website.

# Compression

One of the advanced attributes you can apply to a file or folder is compression. In fact, you can compress an entire NTFS volume. While compression saves disk space, it requires calculation and CPU resources. Compressing a folder or volume that contains files which are regularly updated can negatively impact system performance.

The compression attribute is configurable through Windows Explorer. You can either compress a file or folder or encrypt it; you cannot do both.

## Compressing Files and Folders

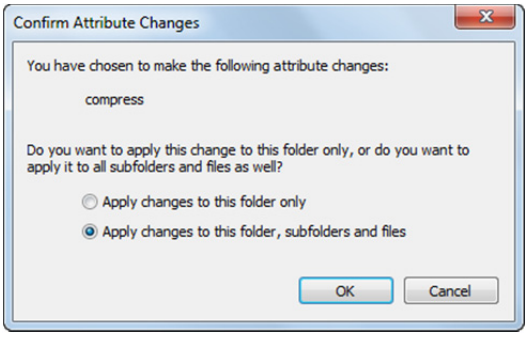
You compress files and folders by turning on the compressed attribute in Windows Explorer. To compress a file:

1. Navigate to the file in Windows Explorer.
2. Right-click the file and select **Properties**.
3. On the General tab, click the **Advanced** button.
4. Check the Compress contents to save disk space check box, then click OK.

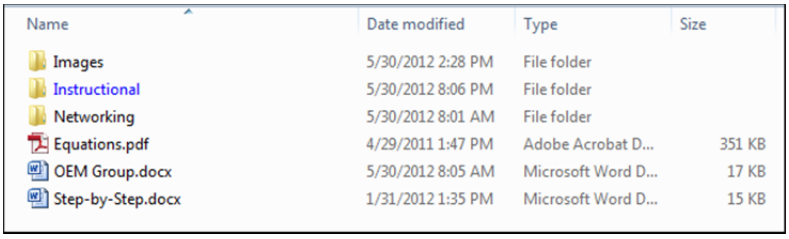
To compress a folder:

1. Navigate to the folder in Windows Explorer.
2. Right-click the folder and select **Properties**.
3. On the General tab, click the **Advanced** button.
4. Check the Compress contents to save disk space check box, then click OK.

When you compress a folder, you are given the option to apply changes to the folder only, or to the folder and its subfolders and files.

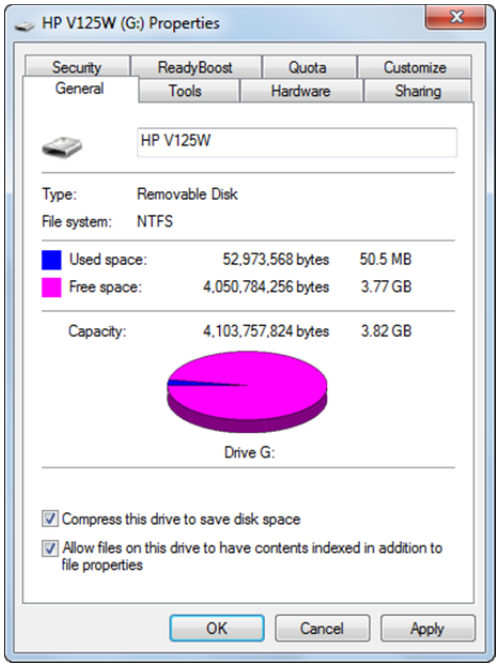


When you compress a file or folder, it displays in blue in Windows Explorer.




To compress a volume:

1. Right-click the volume in Windows Explorer and select **Properties**.
2. On the General tab, select the **Compress this drive to save disk space** check box, then click **OK**.




# Working with Libraries

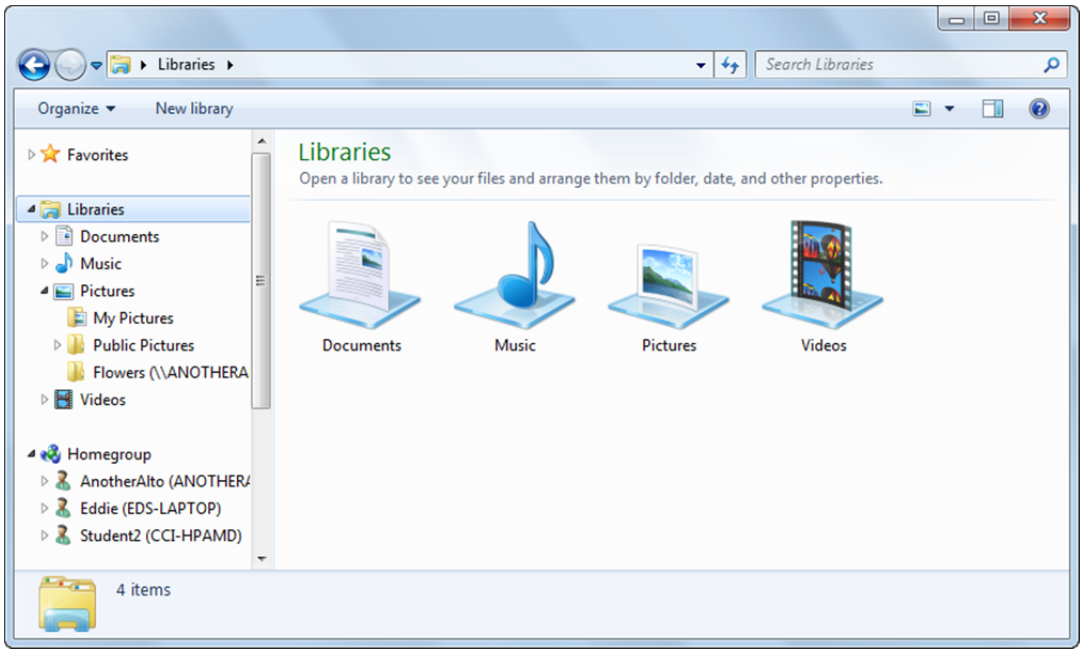
Objective 4.4

Libraries are new in Windows 7. A library is a collection of items, such as files and folders, assembled from various locations. These locations can be on your computer, an external hard drive or someone else's computer. You can use a library to access large amounts of information from a central location.

A library looks and acts like a folder – you can see and manipulate files when you open a library – but the files that appear in a library are not actually stored in the library. Libraries offer a view into multiple folder locations; they monitor the folders that contain your items and allow you to access all of them in one place. For example, if you have picture files stored in various folders on your hard disk and on an external drive, you can access all of your picture files in one place using the Pictures library.

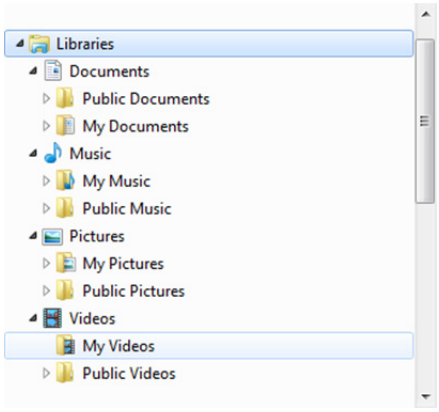
## Default Libraries

When you install Windows 7, four default libraries are created: Documents, Music, Pictures and Videos.




Note that on some systems these libraries may be limited by Group Policy. For example, as a way of discouraging employees from spending their time downloading music or YouTube videos, enterprise systems may not include the Music or Videos libraries.

The default libraries are created for each user profile. They are also created in the public profile. When a user accesses the default libraries, he or she will see folders specific to the user account as well as the public folders.

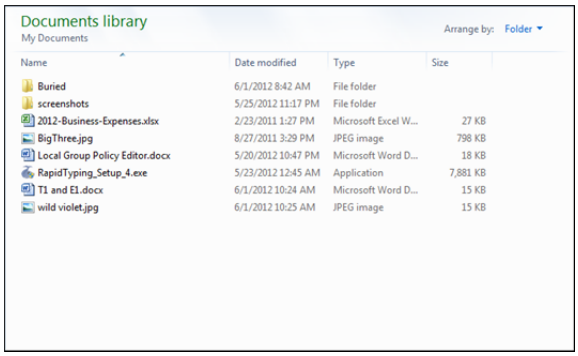


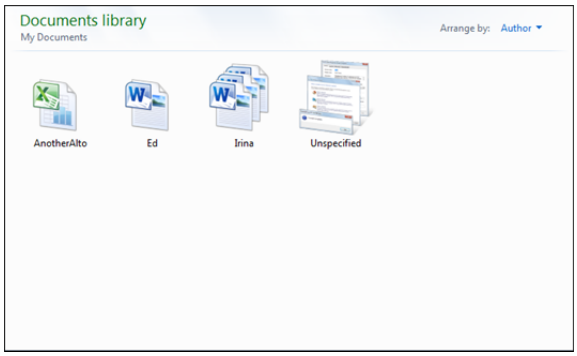

## Using Libraries

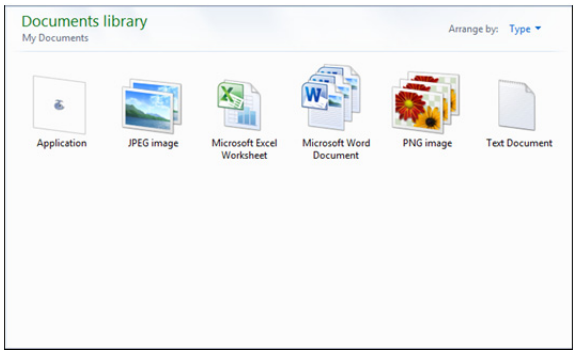
Libraries do more than simply aggregate your files and folders into one location; they allow you to organize and view your collected files and folders in various ways to help you find exactly what you are looking for.

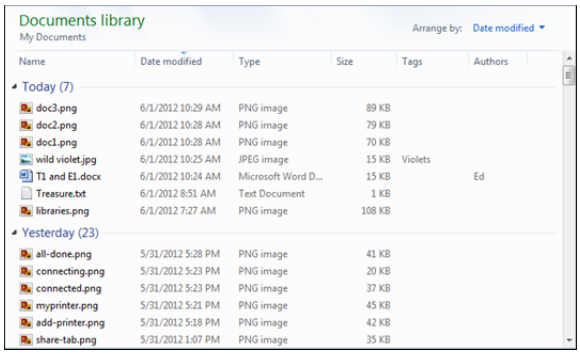
For example, the typical My Documents folder contains a large number of files created by various applications. Have you ever searched for an Excel spreadsheet among hundreds of Word documents and PowerPoint presentations? What if you have picture files in the folder too?

Libraries are designed to help you sort through your files. The following figure shows a few of the ways you can organize the Documents library.

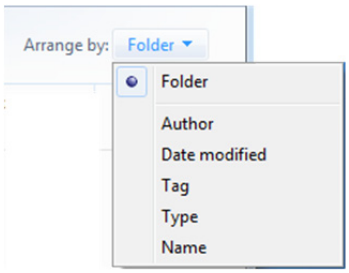



Each library is optimized for the specific type of data it is meant to contain. These optimization settings control the attributes by which you can arrange the items in the library. These attributes appear in the Arrange by drop-down list.

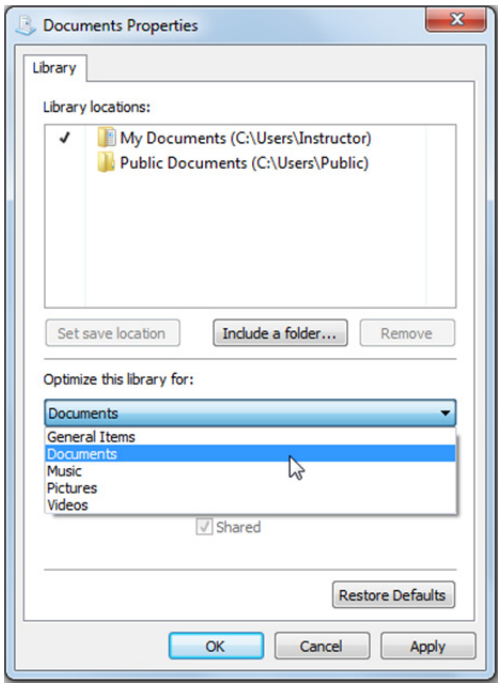



By default, you can arrange libraries by the following attributes:

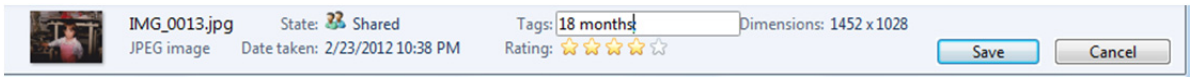
- **Documents** – Folder, Author, Date modified, Tag, Type or Name
- **Music** – Folder, Album, Artists, Song, Genre, Rating
- **Pictures** – Folder, Month, Day, Rating, Tag
- **Videos** – Folder, Year, Type, Length, Name

Selecting options in the Arrange by drop-down list allows you to customize the way your files and folders appear.

If you want to change the optimization settings for a library (thereby changing the attributes that appear in the drop-down list), right-click the library you want to change, then click **Properties**. In the Optimize this library for list, click a file type, and then click **OK**.



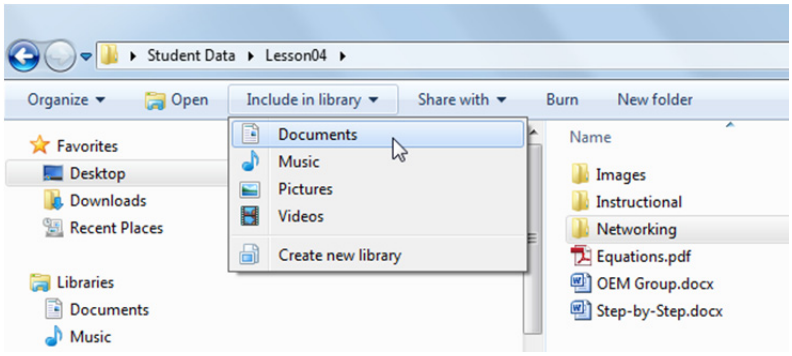

You can also add or update various file attributes while viewing files in the libraries. For example, you can add tags to a picture file, or update the author information for a document. Simply click the attribute in the details pane, type a new value, then click **Save**.



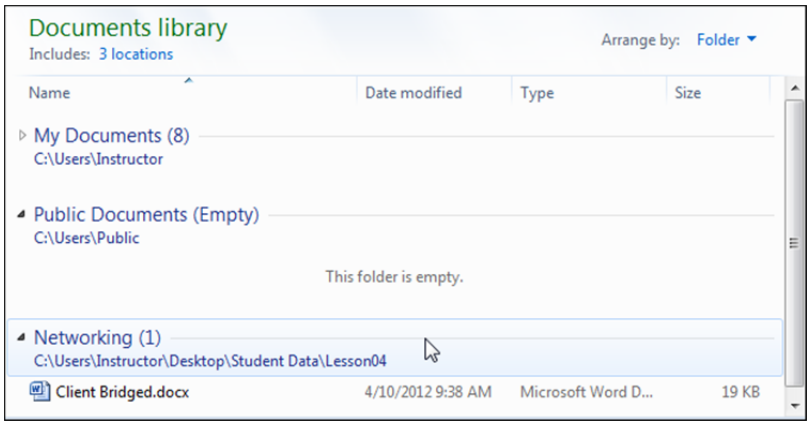

## Including Folders in a Library

You can include multiple folders in a single library.

To include a folder in a library, open Windows Explorer, navigate to the folder you want to include, and click it once to select it. In the Windows Explorer toolbar, click **Include in library**, and then click a library.




The newly added folder displays in the library. Notice that the library indicates how many separate locations are included. In the following figure, the Documents library includes three locations.

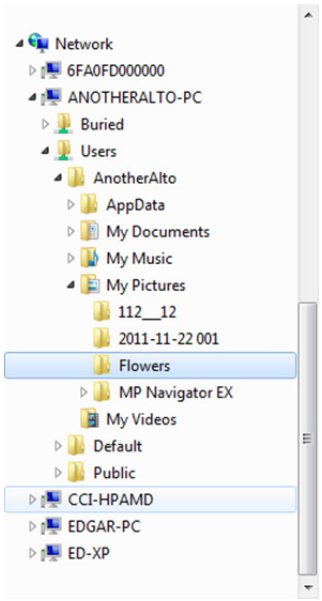



You can use the same method to include folders from external hard drives and some USB drives. If a USB drive appears under the Computer heading in Windows Explorer, then you can include folders from the drive in a library. Some USB flash drives do not appear here, and if they do not, you cannot include folders from them. You cannot include folders from optical drives.

## Including Network Folders

You can include networked locations in a library, but those locations must either be indexed or made available for offline use. Making the folder available for offline use automatically indexes it when it sets it up for synchronization. To make a folder available offline, connect to the network, locate the network folder that you want to make available, right-click the folder, and then click Always available offline. (You learned about using offline files in Lesson 2.)

To include a network folder, open Windows Explorer, then in the navigation pane, click **Network**, navigate to the folder you want to include, click the **Include in library** button in the toolbar above the file list, and then click a library.




If the Include in library option is not available, it means that the network folder is not indexed or is not available offline.

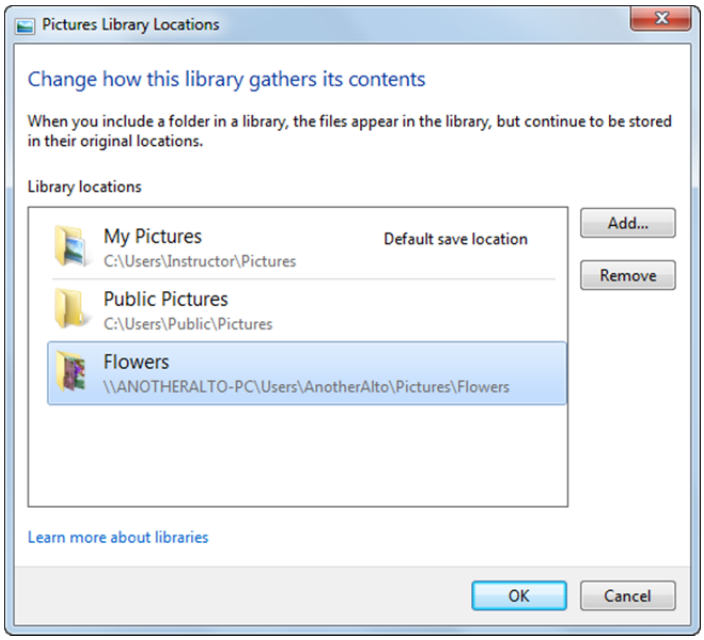
## Removing Folders from a Library

When you no longer want to monitor a folder in a library, you can remove it. Removing a folder from the library does not delete folder from its original location on the disk; the folder is merely removed from the view.

> Removing a folder from a library is distinctly different than accessing a folder through a library and then deleting the folder. Any actions you take directly on a file or folder that you access through a library are carried out on that file or folder on the disk.

To remove a folder from a library, click a library in Windows Explorer, then click the **locations** link.


Clicking the locations link opens the Library Locations dialog box.




Click the folder you want to remove, click the **Remove** button, then click **OK**.

Notice that the Library Locations dialog box also includes an Add button. You can click the **Add** button, navigate to a folder you want to include in the library, select the folder, then click the **Include folder** button to add the selected folder to the library.

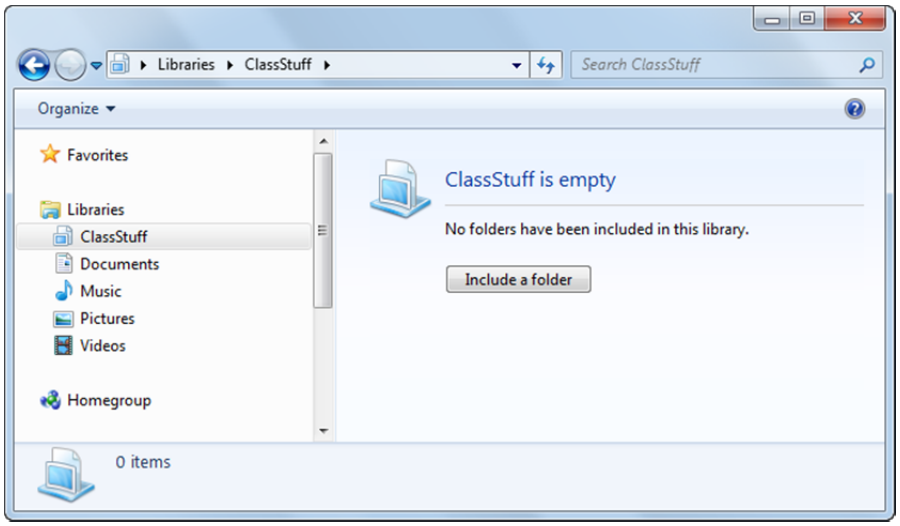
### Default Save Location

Each library has a default save location. The default save location determines where an item will be stored when it is copied, moved, or saved to the library. Only one folder in a multi-folder library can be the default save location.

To change the default save location, click the **locations** link to open the Library Locations dialog box, right-click the folder you want to use as the default save location, select **Set as default save location**, then click **OK**.

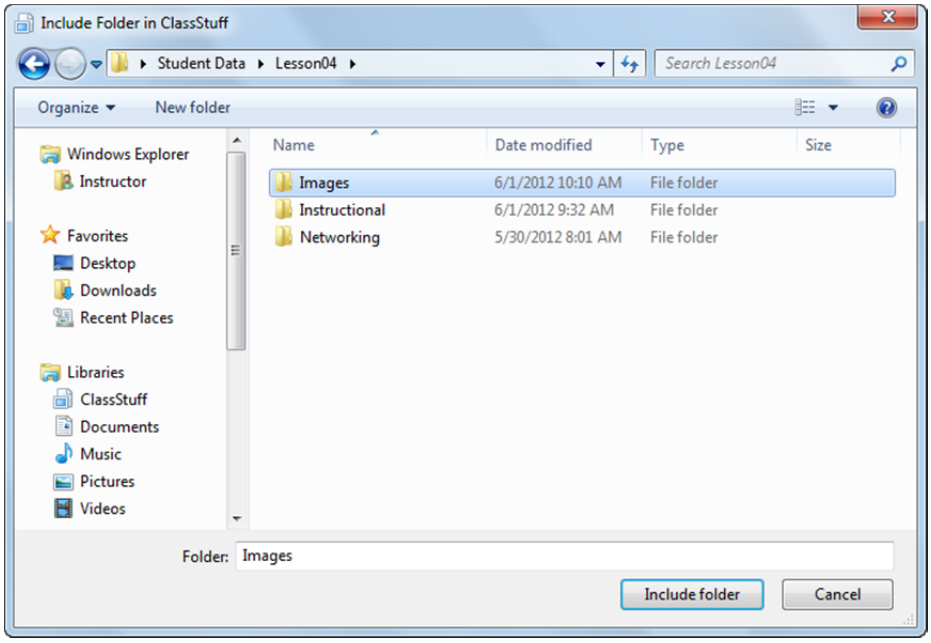
## Creating Custom Libraries

To create a new library, open Windows Explorer and click **Libraries** in the navigation pane. On the toolbar, click **New library**, type a name for the library, and then press ENTER. Double-click the new library to view its contents. The new library is empty.

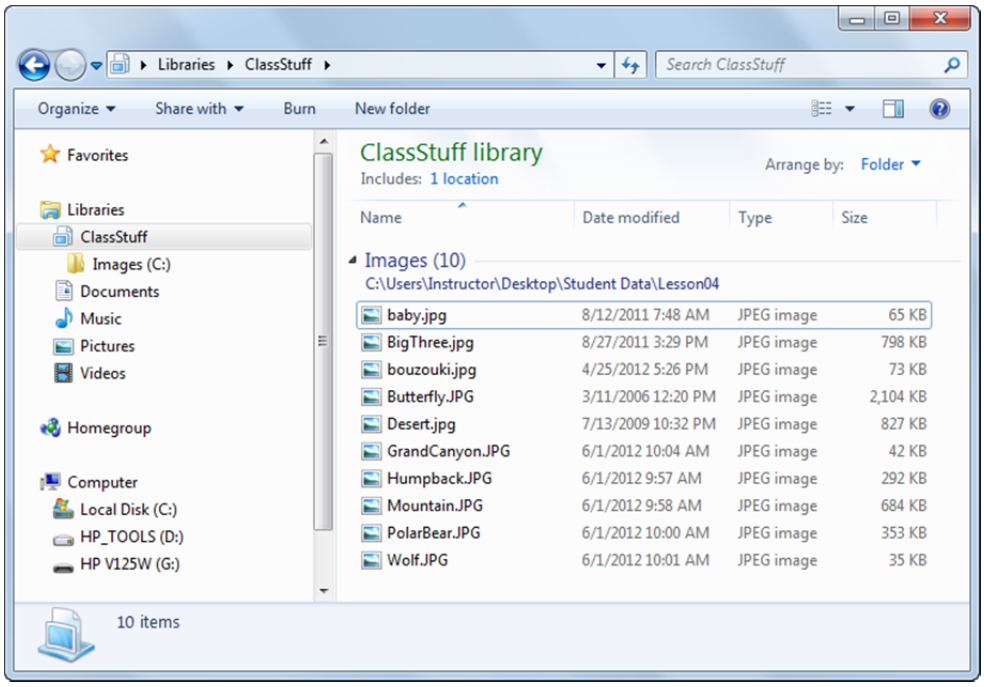



Before you can copy, move or save files to the new library, you must first include a folder in the library so that the library will know where to store the files. This folder automatically becomes the default save location for the library.

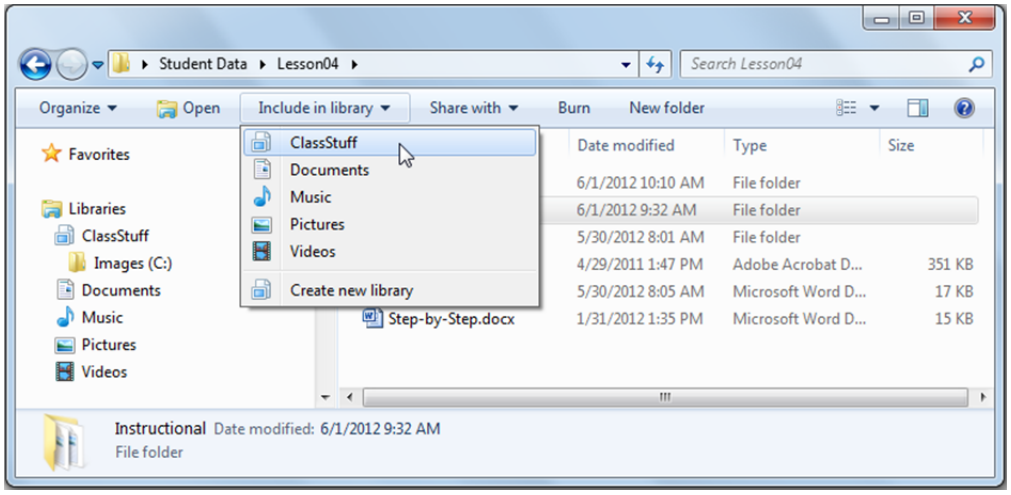
To include the first folder, click the **Include a folder** button, navigate to a folder you want to include, click the folder to select it, then click the **Include folder** button.



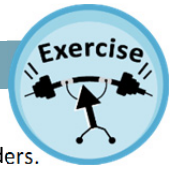

The selected folder is added to the library.




You can add subsequent folders to the custom library in the same manner as you can for the default libraries. The custom library appears in the Include in library drop-down list.




## Exercise 4-3: Working with Libraries




In this exercise, you will work with libraries.

First, you will examine the default libraries, and copy some files to the My Documents and My Pictures folders.

1. Click the **Start** button, click your user account to open Windows Explorer, then click **Libraries** in the navigation pane. Are all four default libraries on your system?
2. In the navigation pane, expand each library to show the included folders.
3. In the navigation pane, click each folder to view its contents. Where are the sample pictures, videos and movies located?
4. Access the *Student Data* folder on the Desktop, open the *Lesson04* folder, then copy the *OEM Group* and *Step-by-Step* document files to the *My Documents* folder.
5. Copy the *heather*, *hyacinth* and *jacaranda* image files to the *My Pictures* folder.

6. In the navigation pane, under Libraries, click the **Documents** library. If necessary, display the Arrange by drop-down list and select **Folder**. The two documents you copied to the My Documents folder should appear, and the Public Documents folder should be empty.
7. In the navigation pane, click the **Pictures** library. You should see the three image files you copied, and the Sample Pictures folder.

Next, you will add folders to libraries, and arrange the files.

8. Navigate to the *Student Data**Lesson04* folder, click the *Instructional* folder, click **Include in library** in the toolbar, then select **Documents**.
9. In the *Student Data**Lesson04* folder, click the *Networking* folder, click **Include in library** in the toolbar, then select **Documents**.
10. Display the Documents library. The files are currently arranged by Folder. Display the **Arrange by** drop-down list, then select **Name**. The files are now arranged in alphabetical order.
11. Arrange the files by a few of the other available attributes. Which arrangements do you think would be most useful for different scenarios?
12. Add the *Student Data**Lesson04**Images* folder to the Pictures library and apply a few of the available arrangements.

Removing a folder from the library does not remove it from the disk.

13. At the top of the Pictures library, click the **locations** link, select **My Pictures**, then click **Remove**. Notice that Public Pictures becomes the default save location. A library must contain a default save location.
14. Click **OK** and confirm that the three flower images no longer display in the Pictures library. Notice also that the My Pictures folder no longer displays under the Libraries heading in the navigation pane.
15. In the navigation pane under the Computer heading, expand the **C:** drive folder, expand the *Users* folder, expand your user folder, then click **My Pictures**. Notice that the three image files are still in the folder.
16. With the *My Pictures* folder selected in the navigation pane, click **Include in library** in the toolbar, then select **Pictures**.
17. Redisplay the Pictures library to confirm that the *My Pictures* folder is now included once again.

Deleting files or folders that you access through a library removes them from the disk.

18. Display the Documents library, then delete the *Kirkpatrick model* document.
19. Navigate to the *Student Data**Lesson04**Instructional* folder on the Desktop. Confirm that the *Kirkpatrick model* document has been deleted.
20. Double-click the **Recycle Bin** icon on the Desktop to open the Recycle Bin, right-click **Kirkpatrick model**, select **Restore** to restore the file to its previous location, then close the Recycle Bin window.
21. Confirm that the file is restored in the *Student Data**Lesson04**Instructional* folder on the Desktop.
22. Redisplay the Documents library if necessary and confirm that the *Kirkpatrick model* document appears in the listing.

You can easily create custom libraries and add folders.

23. In the navigation pane click **Libraries**, in the toolbar click **New library**, type: `ClassStuff` as the name for the new library, then press ENTER.
24. In the contents pane, double-click the **ClassStuff** library.
25. In the contents pane, click the **Include a folder** button, in the toolbar click **New folder**, type: `NewDocs`, then press ENTER to create a new empty folder. The *NewDocs* folder is created under your user profile – c:\Users\<user name>\NewDocs.
26. Click the **Include folder** button to add the new empty folder to the library.
27. Access the *Student Data**Lesson04* folder on the Desktop, click the *Networking* folder, then click **Include in library** in the toolbar. Notice that the ClassStuff library appears in the menu. Select **ClassStuff** in the menu to include the folder in the ClassStuff library.
28. In the *Student Data**Lesson4* folder, copy the *Equations* document to the Desktop.

29. Drag the *Equations* document from the Desktop, to the ClassStuff library, then display the ClassStuff library if necesseary. Notice that the file is copied to the *NewDocs* folder. This folder is the default save location.

Deleting libraries does not remove the folders or files that were included in them. (You can restore deleted libraries from the Recycle Bin.)

30. In the navigation pane, click the **ClassStuff** library, press DELETE, then click **Yes** to confirm the deletion.
31. Confirm that the *Networking* folder and the *Equations* document still reside in the *Student Data**Lesson04* folder on the Desktop.

If you delete one of the default libraries, you can restore it from the navigation pane. However, if you included folders other than the default ones, those are not restored.

32. Delete the **Documents** library, which currently includes the My Documents, Public Documents, C:\Users\<user name>\Desktop\Student Data\Lesson04\Instructional, and C:\Users\<user name>\Desktop\StudentData\Lesson04\Networking folders.
33. In the navigation pane, right-click the **Libraries** heading, then select **Restore default libraries**. The restored library includes the My Documents and Public Documents folders.
34. Delete the *C:**Users**<user name>**NewDocs* folder.
35. Close all open windows.

In this exercise, you worked with libraries.

**MMM**
The inside scoop on libraries

# Lesson Summary

In this lesson, you learned how to manage and share files and folders. You are now able to:

- ☑ Explain disk partitions and logical drives.
- ☑ Describe the file systems supported in Windows 7, including FAT32 and NTFS.
- ☑ Describe how to format a drive and how to convert a drive from FAT32 to NTFS.
- ☑ Explain the purpose and function of HomeGroups and describe how to create and join them.
- ☑ Describe public shares, basic shares and advanced shares.
- ☑ Explain how to map network shares to drive letters.
- ☑ Describe share permissions, NTFS permissions and effective permissions.
- ☑ Explain how to share printers.
- ☑ Explain basic encryption concepts.
- ☑ Describe the function of Encrypting File System (EFS) and BitLocker, and describe how to manage encryption keys.
- ☑ Explain disk compression.
- ☑ Explain the function and characteristics of libraries and describe how to use, customize, create and delete libraries.

**MMM**
Go online for Additional Review and Case Scenarios

# Review Questions

1. Where is information about the size, data content and permissions for each file on a disk stored on an NTFS volume?
   a. In the file allocation table
   b. In the Info library
   c. In the master file table
   d. In the extended partition

2. Why is the NTFS file system preferred over FAT32?
   a. It supports permissions and encryption.
   b. It is a 16-bit file system.
   c. It won't let users compress files.
   d. It prevents file fragmentation.

3. Which of the following is a drawback of HomeGroups?
   a. They are not password-protected
   b. They don't work with XP or Vista
   c. They don't support printer sharing
   d. They don't support Read/Write permissions

4. Mike is accessing a folder on a network share. The share provides Read permission, and the folder Mike needs to access within the share provides NTFS Modify permissions. What permissions will Mike have on the folder?
   a. He will have no permissions at all.
   b. He will have Read permission.
   c. He will have Modify permissions.
   d. He will have Full Control.

5. For what purpose would you use BitLocker?
   a. To encrypt an entire volume
   b. To encrypt individual files and folders
   c. To compress an entire volume
   d. To compress individual files and folders

# Lesson 5: Managing Different Devices

## Lesson Objectives

In this lesson, you will learn how to manage devices connected to your computer. By the completion of this lesson, you will be able to:

- ☐ Explain the purpose and function of device drivers.
- ☐ Describe how compatibility issues between drivers and the operating system can affect the system.
- ☐ Describe how and when to update device drivers.
- ☐ Explain system resources and resource allocation.
- ☐ Explain the features and function of Plug-and-Play technology.
- ☐ Explain when to install third-party software for devices.
- ☐ Describe storage device interfaces.
- ☐ Describe the function of RAID.
- ☐ Describe basic, dynamic and virtual hard disks.
- ☐ Describe the process of using cloud storage.
- ☐ Describe printer ports, printer drivers, the Print Spooler, and the Print queue.
- ☐ Compare and contrast local printers and network printers.
- ☐ Use the Devices and Printers page
- ☐ Explain how to connect and share a local printer.
- ☐ Explain how to connect to a shared printer.
- ☐ Explain how to disconnect printers.
- ☐ Describe how to manage printers.
- ☐ Explain the purpose and function of the Microsoft XPS Document Writer.
- ☐ Describe how printing over the Internet works.
- ☐ Explain video, audio, and infrared devices.
- ☐ Describe how to use Windows Device Manager.

### Exam Objectives

5.1 Connect devices
5.2 Understand storage
5.3 Understand printing devices
5.4 Understand system devices

# Connecting Devices

Objective 5.1

A *device* is any piece of equipment that can be attached to a network or computer, such as a mouse, printer, monitor, game controller, video card, or any other peripheral equipment. Devices may be connected externally through connection ports, or internally through slots or other connections to the system board. Regardless of whether a device is internal or external, a device driver is required to enable Windows to use and manage the device.

Every device requires a device driver to function with Windows.

## Drivers and the Operating System

A *device driver* is a small program that enables a device to communicate with the operating system. A device driver does two things: it "talks" to the hardware device and it "talks" to the operating system, functioning as a type of communication liaison between hardware and software. Rather than accessing the device directly, Windows loads device drivers and calls functions in the drivers to carry out actions on the device.

Device drivers run at the operating system level, and if there is a problem with a device driver, it can cause a system crash. For this reason it is important that you install only drivers that you have retrieved from trusted sources, such as a hardware or software vendor.

Windows operating systems usually come with several device drivers out of the box. When you install a new device that Windows recognizes, Windows will automatically install drivers for the device. The following are just a few of the devices that may not have their device drivers already included with Windows and you have to install the one supplied by the manufacturer:

- Video cards
- Audio cards
- USB-based devices
- Printers

## Locating and Downloading Drivers

Windows will automatically install drivers for you where it can. However, there may be times when you need to use older hardware (because it is what is available) with a new Windows 7 system. For example, you may have an old printer or scanner or removable wireless network interface card (NIC) that was originally designed for use with a Windows XP system. As such, the device most likely shipped with 32-bit drivers, which are compatible with 32-bit Windows 7. But to use these older devices with a 64-bit Windows 7 system, you must find and install 64-bit drivers for them.

In many cases you can visit the device vendor's website to find and download new drivers that will make the device compatible with Windows 7. You may also be able to find drivers at the Windows Compatibility Center, which you learned about in Lesson 1. You can also check the computer manufacturer's website, where you can find drivers specific to your model and configuration.

You may want to check for drivers at the computer manufacturer's site first. Even though manufacturers use third-party brands of devices, in many cases the manufacturer modifies the drivers for use with your specific model of computer. Many manufacturers include driver update utilities on their websites – you need only visit the site and enter your computer make and model. In many cases, the computer manufacturer includes driver update utilities built right into the system and you need only start up the utility and it will evaluate the currently installed drivers and alert and advise you of available and/or recommended updates.

## Installing Device Drivers

To simplify the process of installing device drivers, Windows 7 maintains a large library of signed drivers. This library can be found in C:\Windows\System32\DriverStore. It is created when you first install Windows 7, and updated automatically during the Windows Update process. When you install or connect a new device, Windows will search this driver store first and use the correct driver if one is present. Note that you do not need to be logged on as an administrator if you install a device that uses one of these drivers.

However, you can also install your own device driver to prevent the system from using one from this built-in driver store. The installation instructions for many devices may recommend or suggest that you install the driver from the installation CD or the manufacturer website. If you follow this procedure, you will need administrator rights.

Windows readily accepts device drivers that have been digitally signed by Microsoft or the device manufacturer. If the device driver is not signed, Windows may prevent you from installing the driver. Here is how the system will evaluate a new device driver you try to install:

- **The driver is signed by Microsoft**. It will be installed without any warnings or requests for administrator password. These drivers have been extensively tested by Microsoft for reliability and will not cause your system to crash or become unstable. Therefore, they will be added to the built-in driver store without any complaints.
- **The driver is signed by a third party** (usually the device manufacturer), **and that third party's signature is covered by a certificate which is in the list of Trusted Publishers**. This driver will also be installed without any notifications from the system. These drivers have not been extensively tested by Microsoft for reliability, but you can be confident that they have not been tampered with and that they do not contain a computer virus.
- **The driver is signed by a publisher whose certificate is not in the list of Trusted Publishers**. You must be an administrator to install this driver. If the driver is added to the built-in driver store, then users logged in as standard users can use the driver without any notification about the signature.
- **The driver is unsigned, has an invalid signature, has a digital signature that has been altered, or the certificate cannot be verified by the Certificate Authority**. On a 32-bit Windows system, an administrator will still be allowed to install it. On a 64-bit Windows system, even an administrator will not be allowed to install it.

You should avoid installing unsigned drivers. Device drivers interact directly with the operating system, and a badly written driver poses a much higher risk of causing your system to crash. Therefore if you have an older device for which you are unable to find a signed driver from the manufacturer or Microsoft, you should consider leaving it behind.

If you do decide to install a device driver to override any that may be in the built-in Windows driver store, there are several methods for installing device drivers. Some are provided in executable containers that perform the installation for you. For these, you can simply launch the installation and follow the prompts to install the driver.

Sometimes, drivers come in a compressed archive, such as a ZIP file. You have to extract the files to a folder before you can install the drivers, and the drivers themselves have an .INF file name extension. You can use the Device Manager to install them. (You will learn about the Windows Device Manager later in this lesson.)

Note that in some cases when you are installing multiple device drivers, the drivers must be installed in a specific order. You should always check the documentation or release notes on the manufacturer website for instructions on installing drivers in a specific order. Some manufacturers provide a driver management utility that will automatically detect the drivers you need, and download and install them in the correct order.

## Updating Device Drivers

Over time, the device drivers for your system hardware may become outdated, and vendors often release new, updated drivers. Because an incompatible driver can crash a system, you should carefully consider whether to install updated drivers. Generally, the rule of thumb regarding device drivers is: "if it ain't broke, don't fix it." That is, if your system is running well, the updated driver is likely unnecessary, unless it is a security update.

You should take the following questions into consideration:

- Is the update a security update? If so, then you will probably want to install it.
- Are you having stability or performance problems with the current driver? If so, then the updated driver may remedy the situation. If not, and the update is not security-related, you can probably skip it.

### Drivers and Windows Update

Drivers may be made available through Windows Update, and you can configure a Windows 7 system to automatically download and install device drivers. However, you should take caution when allowing an automated update system to update drivers. Incompatible drivers can cripple a system, and if drivers are installed without your knowledge, it can make it extremely difficult to troubleshoot a driver-related problem should one arise. Manual installation of device drivers is usually preferable to automated installation.

## Drivers in the Enterprise

Poor device drivers can turn a stable machine into an unstable or even unbootable one. In an enterprise environment, it is common practice to track drivers and to update them only when absolutely necessary and only after thorough testing. This is especially important for servers. Servers are usually mission-critical pieces of machinery. The functioning of the enterprise depends on servers to be up and running and available all the time.

Drivers should be:

- Acquired from a reputable source
- Designed for the hardware used in the enterprise
- Supported by the hardware vendor
- Tested thoroughly

It is standard practice to install updated drivers on a test system, and to configure that system as it would be used in the day-to-day business of the enterprise. In this way, the new drivers can be "test-driven" to see how they perform. Only after they are verified to be problem-free will the IT department proceed with installing them on production systems.

Drivers that are compatible with Windows 7 will also be compatible with Windows Server 2008 R2, and vice versa. Both operating systems share the same code base, so you do not need different drivers for the two.

# Communicating with the Processor

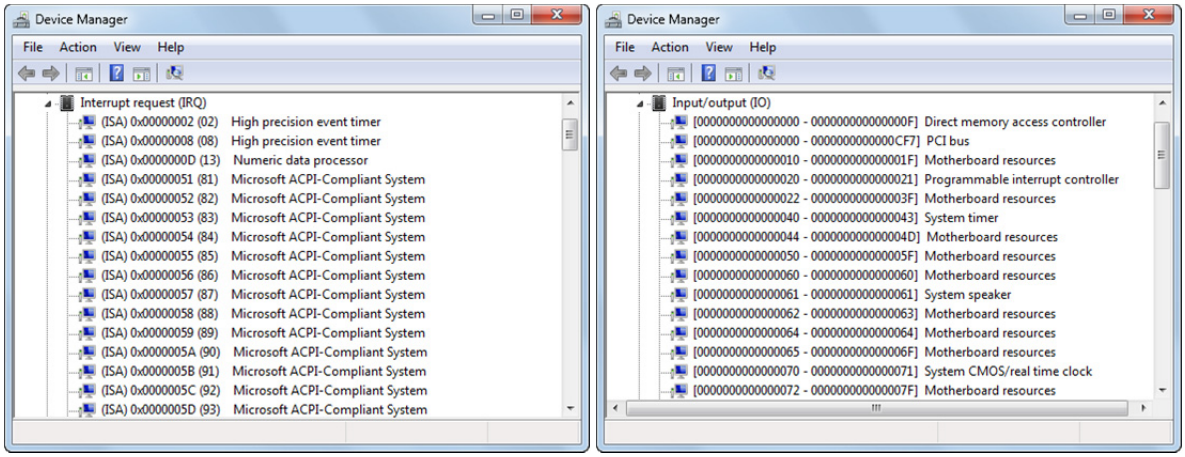
A bus is a circuit or path that carries data between computer components. Essentially, it is a pathway for communication. Buses are created by conductive copper pathways (called traces) embedded or "wired" into the system board. There are several different types of buses inside a PC, and these allow for communications between the CPU and internal components and external devices.

The purpose of a bus is simple; it lets you connect components to the processor. For example, the hard disk, system memory, sound card, and video card all talk to the processor using a bus as a communication path.

Every component inside a computer and every external device attached to a computer must at some point communicate with the CPU. This communication is controlled through **i**nterrupt **req**uest lines, called *IRQs*. IRQs are hardware lines that connect to the bus and allow devices to communicate with the processor. When two devices attempt to use the same IRQ, the result is a hardware error called an IRQ conflict.

While devices use IRQs to get the processor's attention, the processor uses input/output (I/O) addresses to recognize and locate the attached devices. An *I/O address* is a memory location that allows the processor and devices to communicate. Most devices will have at least one unique input/output (I/O) address.

IRQs and I/O addresses are system resources. The allocation or assignment of these communication lines and memory addresses is called resource assignment. At one time, resources had to be assigned manually when you installed new devices. You could check the current assignments in the Device Manager to ensure that you did not make assignments that would cause conflicts.




Devices themselves often had to be configured manually through the use of jumpers or setting DIP switches. Today, however, plug-and-play technology has virtually eliminated the need for manual configuration.

# Plug-and-Play (PnP)

Plug-and-Play is a technology that allows for the automatic configuration of hardware resources. It enables Windows to detect and configure hardware with little or no user involvement. With PnP, you simply plug the device in and let the OS do the configuration work.

PnP monitors the bus and detects and responds to the presence of new devices and components. For example you can insert a new video card into an expansion slot, close up the case and power on the system. When Windows boots up, PnP will detect the new hardware, find the right driver from its built-in driver store and install it, allocate resources to the new card and create any required Registry entries. If windows can't find an appropriate driver, it will launch the Add New Hardware wizard and allow you to specify where suitable drivers are located.

The Plug-and-Play Manager is the component responsible for determining the hardware resources (e.g., I/O ports, IRQs, memory locations) requested by each device and assigning hardware resources appropriately. The PnP Manager reconfigures resource assignments when necessary, such as when a new device added to the system requires resources already in use.

Plug and Play makes it easier to add and configure hardware on a computer running Windows without special user knowledge of hardware configurations. For Windows 7, certain classes of devices are fully supported for PnP, including PCI, PCI Express (PCIe), ExpressCard, and PCMCIA mounted cards, as well as any device that can be connected using USB or Firewire. Older devices that connect using the parallel or serial port may be PnP compatible but most are not.

Some PnP devices are designed to be hot-pluggable; that is, they can be inserted while the system is running and you do not need to reboot the system. For example, you can insert a USB flash drive into a USB port and Windows will automatically detect it, load any necessary drivers, and allocate system resources without requiring a reboot. Other devices are designed to be hot-swappable; these components can be removed and replaced by a similar component without the need to shut down the system. For example, many servers have RAID drives (described in more detail below) that can be removed if they fail during operation and replaced with a new RAID drive. Since the server is not shut down during this entire procedure, it continues running without any loss of service. This is a necessity for banks, airlines, and other companies that need to maintain continuous round-the-clock services.

However, you need to understand that only certain types of devices are designed to be hot-plugged or hot-swapped. For example, you must never open a computer case and touch any of the components inside while the power is on; you will most likely get an electrical shock. Hot-pluggable and hot-swappable devices have handles, latches, or connectors on the outside of the computer that are designed to be inserted or removed easily.

### Connecting Plug-and-Play Devices

When a new PnP device is detected, the user is prompted with the Found New Hardware dialog box and three driver installation options:

| | |
|---|---|
| **Locate And Install Driver Software** | Selecting this option begins the installation process. |
| **Ask Me Again Later** | Leaves the device uninstalled. No configuration changes are made. If the device is still plugged in the next time the user logs on, the dialog box will appear again. |
| **Don't Show This Message Again For This Device** | Configures the Plug and Play service to not install the driver for the device, and the device is not made functional. To complete the installation of the device driver, you must detach the device and reattach it so that it can be detected again. |

Note that the user must be logged on as an administrator to install devices.

### Connecting and Disconnecting Printers

In Windows 7, printers that are directly connected to a PC with a USB cable are treated as plug-and-play devices. Windows 7 automatically detects and installs the printer when you connect the USB cable. However, to use the rich printer features, it is better to use the drivers that come on the vendor-supplied installation CD. Connecting and disconnecting printers is treated in more detail later in this lesson.

## Installing Third-Party Software for Devices

Some hardware may benefit from the installation of additional software. While a device driver is required for the hardware to work, the additional software may add extra capabilities or features. For example, you can install the device driver for a wireless network adapter card and use it with the built-in Windows 7 networking features to obtain access to wireless networks. However, you can download and install custom management software for the wireless network adapter and use this software to manage wireless connections or expand the capabilities of the network adapter card by adding encryption protocols.

It is important to remember that most third-party software for devices is optional. While these software options can make the devices easier to use, you should consider how they affect the performance of the system before installing them. These extra software options are often referred to as bloatware. Installing and running too many of them can degrade performance while offering little true "enhancement."

Compelling reasons to install third-party software for devices include the following:

- to gain extra features
- to improve usability
- to improve performance
- to increase security

# Understanding Storage

Objective 5.2

Data in a PC is stored on various types of media – hard disks, tape, optical disks and flash drives. The primary storage location, however, is on one or more hard disks. The storage media used in a hard disk can be magnetic or flash-based (solid state).

Each hard disk is contained within a hard disk drive and is connected to a hard disk controller which enables the CPU to communicate with the hard disk.

Hard disk drives can be internal (housed within the system) or external. Regardless of the type of drive used, hard disk drives connect to the PC via one of several standard interfaces. An interface is a communication standard that defines how data flows to and from the disk drive.

## Storage Device Types

The connection interface is linked to the type of hard drive device you are using. Several hard drive types have been developed over the years. The ones still in use today are described in the following table:

| Interface | Description |
|---|---|
| **IDE (PATA)**<br>**Integrated Drive Electronics** | The official name is the AT Attachment (ATA) interface. These drives communicate data in parallel, and are sometimes referred to as Parallel ATA or PATA. Supports internal drives only. The IDE interface is commonly used for optical drives; however, the newest computers no longer use it for hard drive connections. Newer systems use SATA drives. |
| **SATA**<br>**Serial ATA** | Serial ATA communicates data in serial, uses lower voltage than the IDE interface, and provides faster speeds than IDE. SATA drives range in speed from 1.5 Gbps (SATA 1.0) to 6 Gbps (SATA 3.0). They are supported in both servers and desktop systems. |
| **eSATA**<br>**External Serial ATA** | External SATA (eSATA) drives may be connected using external connectors on the computer. This standard competes with FireWire and USB for speed, but requires a separate power connector. Provides speed up to 3 Gbps. |
| **SCSI**<br>**Small Computer Systems Interface** | The SCSI standard is not limited to hard disk drives and other mass storage devices. It supports a wide variety of other devices, such as printers and scanners. Supports internal and external drives. Depending on the version, SCSI can use a parallel or a serial interface. SCSI drives come in many versions and support speeds up to about 5 Gbps. SCSI commands can be sent across TCP/IP networks when the iSCSI protocol is used. |
| **iSCSI** | iSCSI is a protocol used to transmit storage data information across IP networks. iSCSI allows you to send SCSI commands over a local area network, a wide area network, or the Internet, thereby allowing you to store information on drives located anywhere in the world (as long as the drive is accessible through a connected network). iSCSI is used to manage storage over long distances. The speed of the data transmission is controlled by the speed of the network speed. For example, in a 10-GB Ethernet LAN, data is transferred via iSCSI at 10 Gbps. |
| **IEEE 1394**<br>**FireWire** | A serial bus interface standard for high-speed communications and data transfer. IEEE 1394 technology that is based on the SCSI standard and is frequently used in personal computers, digital audio, digital video, automotive and aeronautics applications. Provides speeds of 400 Mbps (FireWire 400), 800 Mbps (FireWire 800), 1.6 Gbps (FireWire S1600) and 3.2 Gbps (FireWire S3200). As with USB devices, FireWire devices can be plugged in and expected to work. You seldom need to load device drivers. FireWire is also sometimes used for direct system-to-system connections for high-speed data transfer. |
| **USB**<br>**Universal Serial Bus** | Used with external devices. USB can connect computer peripherals such as mice, keyboards, digital cameras, printers, personal media players and flash drives. USB supports self-configuration of devices, as well as the ability to hot plug devices. USB ports also deliver power (up to 5 volts at 6 amps – or a total of 30 watts) to connected devices. The original specification (USB 1.1) provides a transfer rate of 12 Mbps/1.5 Mbps for slow devices. Communication is half-duplex (that is, the device can upload or download, but cannot do both simultaneously). |

| | |
|---|---|
| **USB 2.0** | Maximum transfer rate of 480 Mbps. Communication is half-duplex. USB 2.0 is the current de facto standard. |
| **USB 3.0** | Maximum transfer rate of 4.8 Gbps. Communication is full-duplex and USB 3.0 includes power management which allows devices to move into idle, suspend and sleep modes. USB 3.0 is not yet in wide use, although a few companies have begun implementing the standard on their mass storage devices, video capture cards and expansion cards. |

# Disk Types

As you learned in Lesson 4, Windows 7 supports the FAT, FAT32 and NTFS file systems. The advantage to using NTFS is that it offers built-in security through permissions and encryption. You can use Encrypting File System (EFS) to encrypt individual files and folders on an NTFS volume, and BitLocker to encrypt entire NTFS volumes.

# A Few Words about RAID

Before moving on to the topic of drive types, it will be helpful to understand the function and characteristics of RAID. RAID stands for Redundant Array of Inexpensive Disks. (Later, this was changed to Redundant Array of Independent Disks.) RAID is a set of standards that allows you to configure a set of two or more physical drives to act as a single entity.

RAID can be implemented using hardware or software. When used as a hardware implementation, a RAID-capable hard drive controller manages the physical drives. All of the RAID processes are handled by the controller and are typically configured through a special application provided by the hardware vendor. Some network operating systems such as Windows 7 offer RAID software support. In software-based RAID, the operating system itself handles the RAID configuration, and standard hard drive controllers can be used.

RAID is most commonly used today to protect data by providing fault tolerance through data redundancy. Fault tolerance refers to the ability of a system to respond gracefully to an unexpected hardware or software failure.

RAID is characterized by levels. The most frequently used RAID levels include:

- **Level 0** — disk striping (does not provide fault tolerance).
- **Level 1** — disk mirroring (provides fault tolerance, but not to the extent of RAID 5).
- **Level 5** — disk striping with parity (the most often-used form of fault-tolerant RAID).

## RAID 0: Disk Striping

A stripe set is a collection of physical drives that have been configured to act as a single logical drive. RAID Level 0 causes each file written to the stripe set to be divided into pieces, and then each piece is written to a separate physical drive in the stripe set. RAID 0 splits data evenly across two or more disks, which results in faster system performance because the activity of reading data from and writing data to hard drives is much slower than CPU or on-board RAM operations. However, this approach has a higher risk of data loss caused by a failure of any of the drives.

## RAID 1: Disk Mirroring

Disk mirroring duplicates all write requests on two hard disks. When you use mirroring, two sets of writes occur for each write procedure. Data is written to the primary drive when a write request is issued and is then copied to the mirrored drive, providing a mirror image of the primary drive. In this way, an automatic backup is created. If one of the hard drives fails, all data is available on the other. Mirroring can be implemented using the same physical hard drive controller for both drives.

## RAID 2 to RAID 6: Disk Striping with Parity

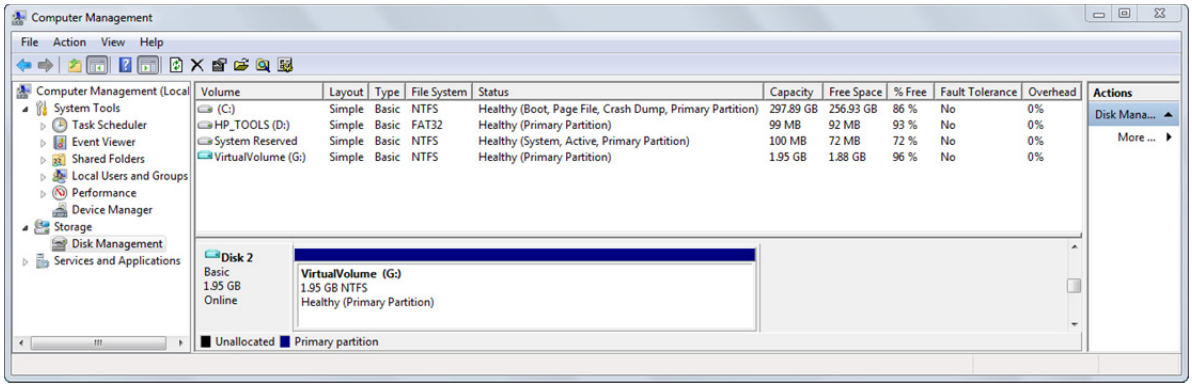
Of these five (RAID 2, 3, 4, 5, and 6) different designs, RAID 5 is the most common. All of these designs use three or more hard disks. As data is written to the stripe set, parity information is also written to the disks, making it possible to detect and correct disk errors if any one disk in the RAID array should fail. Parity is a mathematically calculated value that can be used to regenerate missing data.

Although a portion of each write request is written to a separate physical drive in the stripe set, the parity information is calculated on the entire file, and is written to a completely separate physical drive. For each file written, parity information never resides on the same physical disk as file information for which the parity is calculated.

# Drive Types

In Lesson 4, you were introduced to primary and extended partitions. You learned that primary partitions can be used to start an operating system, and that a basic disk can contain up to four primary partitions, or three primary partitions and one extended partition. An extended partition can hold one or more logical drives. Each logical drive is a volume, and each is assigned its own drive letter. Logical drives function like primary partitions except that they cannot be used to start an operating system.

This section introduces the concepts of basic, dynamic and virtual disks. All types of disks can be managed using the Disk Management snap-in.




## Basic Disks

A basic disk is a physical disk that can contain primary partitions, an extended partition, and logical drives. Partitions and logical drives on basic disks are known as basic volumes. Basic disks provide the basic features and functions required for typical storage tasks. However, they do not support software-based RAID.

The following tasks can be performed on basic disks, but cannot be performed on dynamic disks:

- Creating and deleting primary or extended partitions
- Creating and deleting logical drives
- Formatting partitions
- Marking partitions as active

## Dynamic Disks

A dynamic disk is a disk that provides features that basic disks do not, such as the ability to create volumes that span multiple disks. These are called spanned volumes. You can also use dynamic disks to create fault-tolerant (mirrored) RAID 1 volumes.

To change a basic disk into a dynamic disk, follow these steps.

1. In the Disk Management snap-in, right-click the basic disk you want to convert.
2. Click **Convert to Dynamic Disk**.
3. Follow the instructions on the screen.

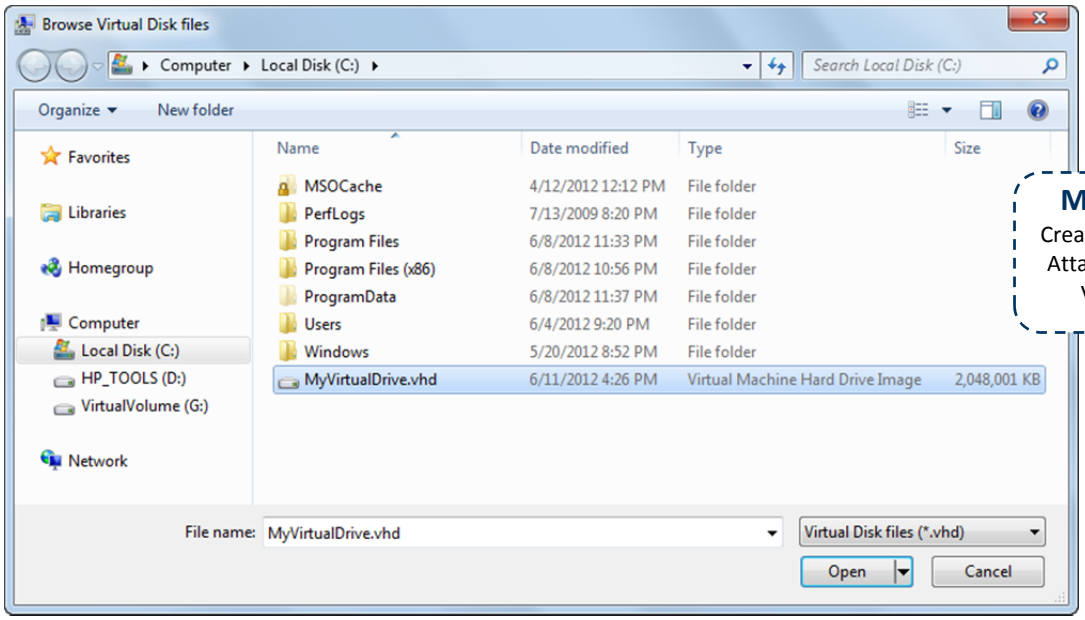
Note that dynamic disks cannot be changed back to a basic disk without loss of data. You must first delete the volume.

*Dynamic disks are not supported on portable computers, removable disks, or detachable disks that use USB or FireWire interfaces.*

## Virtual Hard Disks (VHDs)

Virtual hard disks (VHDs) are used with virtualization systems such as VMware and Hyper-V. VHDs are single data files on a physical hard disk that are used as drives within virtual machines.

Windows 7 and Windows Server 2008 R2 allow you to attach a VHD file as a hard drive within the operating system as if it were a physical drive. You can also boot an operating system from a VHD file that is stored on the local disk. The following figure shows a virtual hard disk file in Windows Explorer.




**MMM**
Creating and Attaching a VHD

A particularly useful feature of VHDs is that you can detach them from one machine and then attach them to another. All the files contained on the VHD are then instantly available on the system to which the VHD is attached.

# Storing Items in the Cloud

*Cloud computing* is the practice of using applications or storage space on the Internet rather than on your own computers and servers. That is, you can use hosted applications and services offered by a third party and run almost entirely from one or more servers that reside on the Internet. All that is required to use cloud computing services is a Web browser and an Internet connection; no other software needs to be installed.

Although the applications reside on remote servers, users can store files on a local drive or on a remote system. The remote, cloud-based applications do the majority of the processing work. The local browser is responsible for rendering the applications. Even though only a Web browser is used, the cloud-based applications can be as robust as those you would install on your local system.

Common cloud computing services include:

- Document creation (word processing, slide shows, spreadsheets, forms) and collaboration.
- File storage, backup and management services.
- File sharing and project management services.
- Instant messaging (IM) and email services.

Many cloud providers offer integrated services – their applications and data storage and email and messaging applications are designed to work seamlessly with one another.

## Windows Live

Windows Live is the brand name for a set of services from Microsoft. Many of these services are Web applications, accessed through a web browser.

Windows Live Essentials is a suite of freeware applications by Microsoft that offers integrated and bundled email, instant messaging, photo-sharing, blog publishing, security services and other Windows Live entities. Essentials programs are designed to integrate well with each other, with Microsoft Windows, and with other Windows Live web-based services such as SkyDrive and Hotmail, so that they operate as a "seamless whole."

The Windows Live Essentials suite includes the following applications:

- Windows Live Family Safety
- Windows Live Mail
- Windows Live Mesh
- Windows Live Messenger
- Windows Live Messenger Companion
- Windows Live Movie Maker
- Windows Live Photo Gallery
- Windows Live Sign-in Assistant
- Windows Live Writer
- Bing Bar
- Microsoft Outlook Hotmail Connector
- Microsoft Silverlight

Windows Live Essentials applications can be installed on Windows Vista SP2, Windows 7, Windows Server 2008 SP2 or Windows Server 2008 R2.

To use any/all of these applications, a Windows Live ID is required. A Windows Live ID is composed of an email address and password. You can then use the Live ID to sign in to Hotmail, Xbox Live, and all Windows Live services (including SkyDrive and Messenger).

If you use Hotmail, Windows Live Messenger, or Xbox Live, you already have a Windows Live ID. If you don't have a Windows Live ID, you can create one by completing an online form at the Windows Live Signup page at https://signup.live.com/signup.aspx?lic=1. You can also create a Hotmail or Live.com email account at the same time.

## Windows Live SkyDrive

**MMM**
Productivity with Windows Live

Windows SkyDrive is an online storage service provided as part of Windows Live. Using the cloud to store files provides several benefits:

- Store files for access from anywhere.
- Create backups of important files.
- Share files with others.

When you download SkyDrive onto a PC or Mac, a desktop SkyDrive folder is automatically created. Any file or photo you put in this folder will be automatically synced to your other devices that have SkyDrive. This means that you can use your phone or tablet to get the files and photos you've saved to SkyDrive, and all your SkyDrive files will be synchronized on all your computers and devices. You simply download and install the app for each device.

SkyDrive also includes a "Fetch your files from anywhere" feature that allows you to (remotely) access your PC from any of your devices and browse through files on the PC just as if you were sitting in front of it.

SkyDrive offers the following storage and management features:

- Free storage space – 7 GB are included free, and you can add more for a yearly fee.
- Organization – data can be organized into top-level folders and subfolders that you create and name.
- Security – you can set permissions for each folder, and all uploads and downloads are encrypted.
- Fault tolerance – multiple copies of each file are saved on different servers and hard drives to help protect data from hardware failure. When selecting a cloud storage provider for a business storage solution, it is important to choose a vendor with a data backup guarantee.
- Flexibility – you can upload files as large as 2 GB in file size and then copy, move, delete, rename and caption files after uploading them.
- Sharing – you can share links directly to your SkyDrive folders so that others can access the data. All others need is a web browser. This saves you the trouble of having to send multiple, possibly large, file attachments via email.
- Synchronization – you can synchronize the data in your SkyDrive folder to your local Windows 7 machine so that it is automatically updated wherever you make changes.
- Integration with Microsoft Office – share your Office documents, spreadsheets and presentations on your SkyDrive folder, and others can view and edit the files using free Office Web Apps if they don't have Office installed), or using their installed Office programs. If multiple users have Office 2010 installed, they can collaborate on documents. That is, multiple people can edit a document at the same time and see each other's changes. SkyDrive also maintains a version history for the previous 25 versions of a document.
- Integration with social networking applications – you can share your SkyDrive files with contacts on Facebook, Twitter, Gmail and LinkedIn.

### System Requirements for SkyDrive

Following are the system requirements for Windows Live SkyDrive:

- **Operating system**: 32- or 64-bit version of either Windows 8 Consumer Preview, Windows 7, or Windows Vista with Service Pack 2 and the Platform Update for Windows Vista, or Windows Server 2008 R2, or Windows Server 2008 with Service Pack 2 and the Platform Update for Windows Server 2008, or Mac OS X 10.7 (Lion).
- **Processor**: 1.6 GHz or higher, or Intel-based Mac computer
- **Memory**: 1 GB of RAM or higher
- **Resolution**: 1024 × 576 minimum
- **Internet connection**: High-speed Internet access is recommended

### OneNote to SkyDrive

Microsoft OneNote 2010 is a digital notebook that provides a single place where you can gather and organize notes and information. You can gather and organize text, pictures, digital handwriting, audio and video recordings, and you can use OneNote's search capabilities to find what you are looking for quickly. You can also share notebooks with other users. OneNote 2010 is an integrated part of Microsoft Office 2010.

OneNote to SkyDrive is a feature that allows you to synchronize OneNote notebooks with SkyDrive.

## Windows Live Mesh

Windows Live Mesh is an Internet-based file synchronization application. It is designed to allow files and folders between two or more computers to be in sync with each other or the Web via Windows Live SkyDrive. Windows Live Mesh also enables remote desktop access via the Internet.

You can use Windows Live Mesh to:

- Sync folders on SkyDrive.
- Sync program settings so that they are duplicated on all computers. This includes the synchronization of Internet Explorer favorites, and Microsoft Office style templates.
- Sync data between computers using Windows Live as the intermediary.
- Connect to your PC from a remote location.

## Exercise 5-1: Storing Items in the Cloud with Windows Live

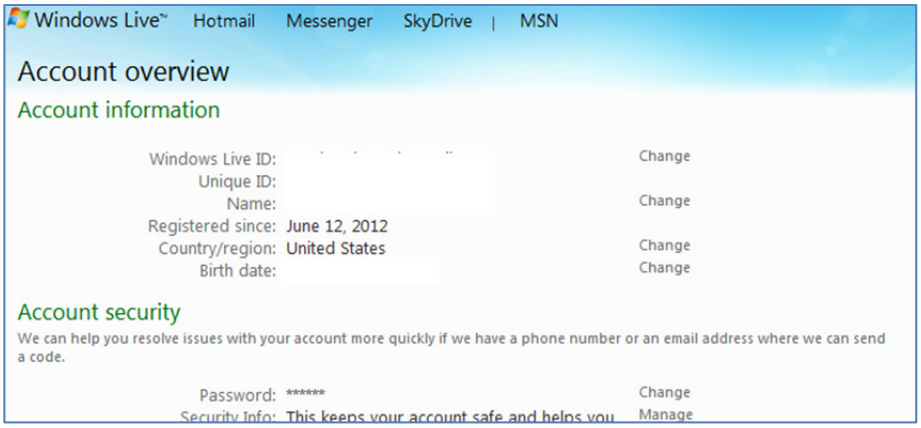

In this exercise, you will explore SkyDrive.

First, you will create a Windows Live ID if necessary. If you already have a Windows Live ID, skip to Step 6.

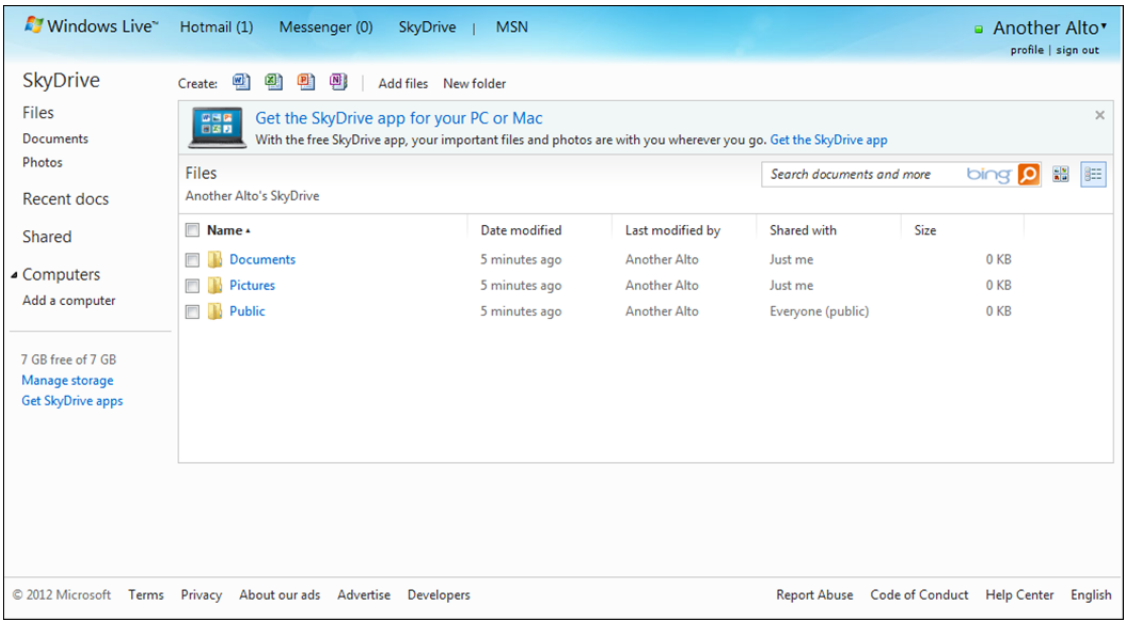
1. Open a web browser and navigate to https://signup.live.com.
2. On the Create Your Windows Live ID page, click the **Or get a Windows Live email address** link.
3. Fill out the form as directed on the page to create a new Windows Live ID and Hotmail account. Write down your user name and password – you will need them for signing in to Windows Live.
4. When you have completed the form click **Done**. When your account has successfully been created, you will be taken to your Hotmail inbox.
5. Sign out of Hotmail.

Sign in to SkyDrive. If you are using a pre-existing Windows Live ID you may not see all of the security screens that are shown in this exercise. Skip through steps as necessary based on the screens you do see.

6. Navigate to login.live.com.
7. Enter your new Windows Live ID (including the "@hotmail.com") and password and click **Sign in**. The Account overview page appears.




8. In the navigation bar across the top of the page, click **SkyDrive** to access your SkyDrive page. The default folders are already prepared for you, and you should have 7 GB of free space. (Note: If the default folders have not been created, you can create them at any time.)

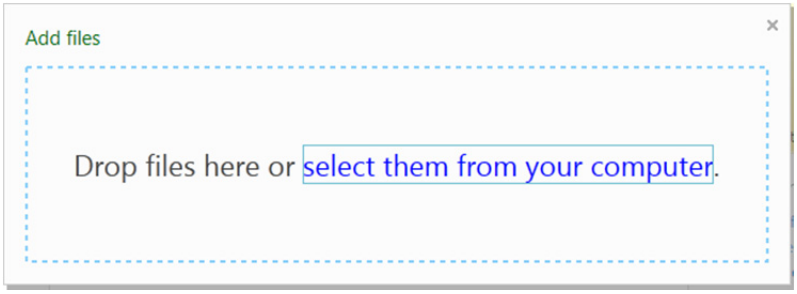



You can drag folders from your local system right into SkyDrive.

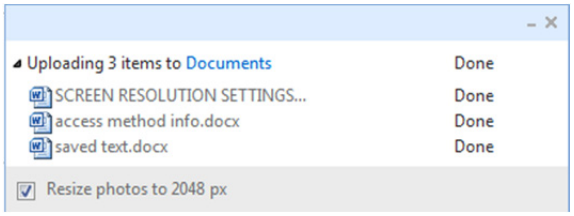
9. Open Windows Explorer, make sure that the window is not maximized, navigate to the *Student Data* folder on the Desktop, then navigate to the *Lesson05* folder.

10. Click on the **Documents** link in SkyDrive to navigate into that folder, and then click **Add files**.

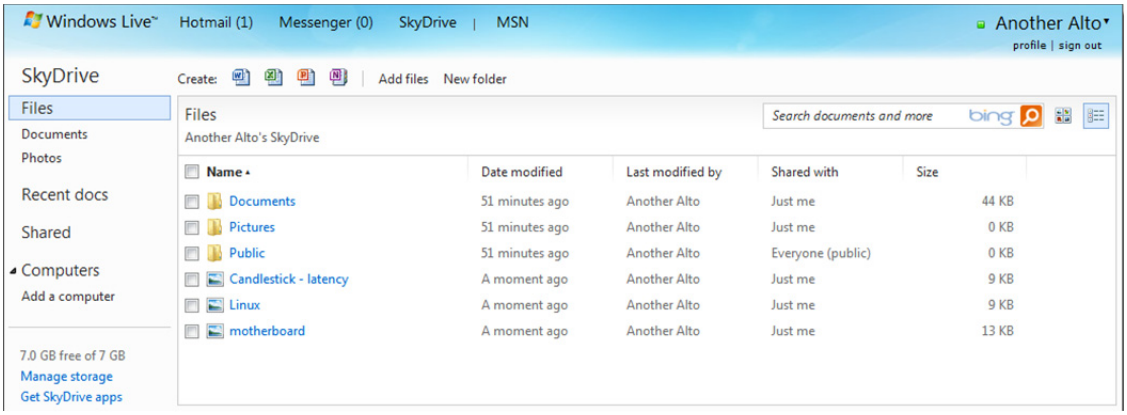
The Add files drop box may appear in front of the SkyDrive.



11. Arrange your windows so that you can see both Windows Explorer and SkyDrive, then drag the three Word documents from the *Lesson05* folder in Windows Explorer to the Add files drop box on SkyDrive. (If the Add files drop box did not appear, drag the Word documents onto the Documents folder in SkyDrive.) A small window opens to show the progress of uploading the selected files.



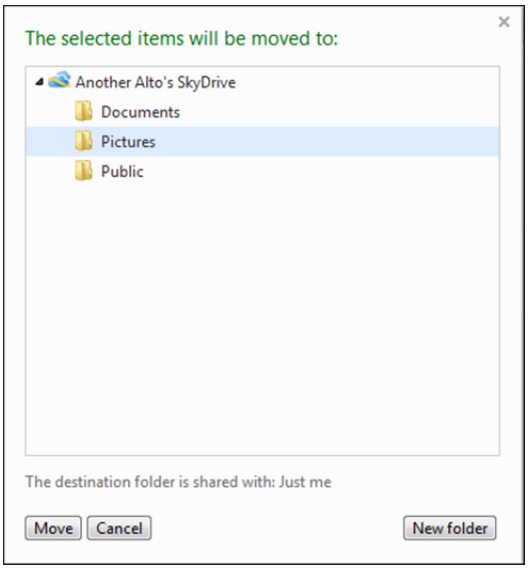

12. Close the upload window if it does not close itself automatically.
13. In SkyDrive, click one of the documents to open it.
14. Click the browser **Back** button twice to view the SkyDrive folders. Alternatively, you can click the close icon located at the upper right of the Microsoft Word Web App window, and then click the **Files** link in SkyDrive to view all folders.
15. Next, click **Add files** in SkyDrive again and drag a few of the image files from the *Lesson05* folder in Windows Explorer to the Add files drop box. The files should appear similar to the following figure.




16. If necessary, click the **Files** link in SkyDrive to view all files at this folder level in SkyDrive. If **Documents** is selected, then only document-type files are displayed.

You can also move files on SkyDrive.

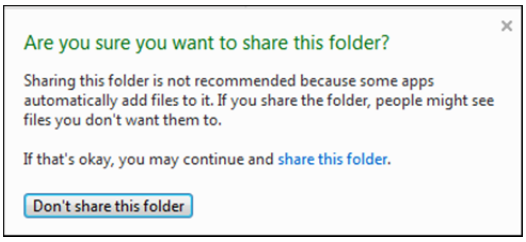
17. If you do not have a Pictures folder in SkyDrive, click **New folder** to create a new folder and change the name to `Pictures`. Click the check box next to it to turn it off.
18. In SkyDrive, select the check boxes for the three image files, then in the right area of the page, click the **Move to** link.
19. In the box that appears, click the *Pictures* folder to specify that you want to move the images to the SkyDrive Pictures folder.



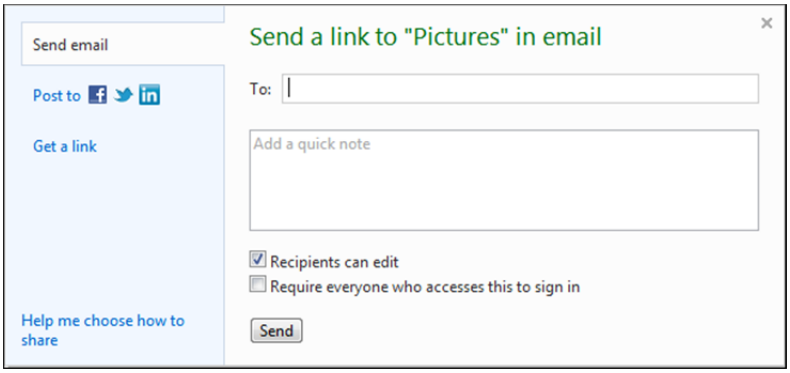

20. Click the **Move** button to move the files.
21. In SkyDrive, click the *Pictures* folder to view its contents, and then click the browser **Back** button.

You can specify to share files and folders on SkyDrive.

22. Select the check box for the *Pictures* folder, and then look at the right side of the page under Sharing. The folder is currently not shared.
23. Click the **Share** link. SkyDrive may display the following message asking if you are sure you want to share the folder.

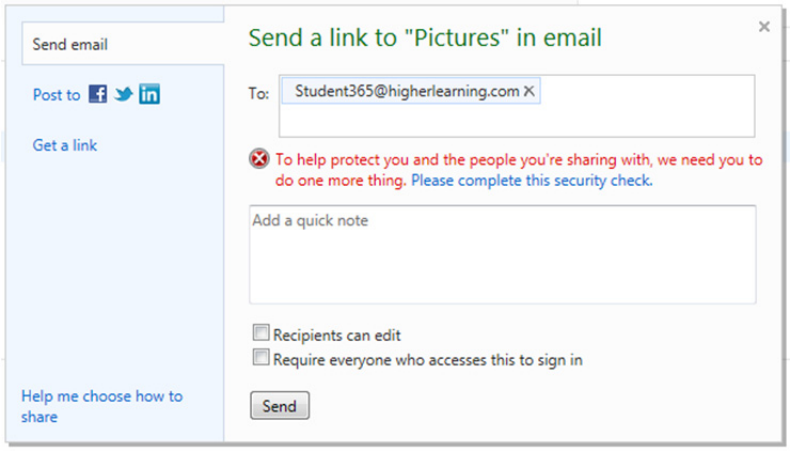



24. In the message box, click the **share this folder** link. SkyDrive gives you the option of sending an email link to the people you want to share with, sharing the folder on Facebook, Twitter or LinkedIn, or generating a link that will allow recipients to view, or to view and edit your shared files. You can then copy and paste the generated link into an email message that you compose and send on your own.



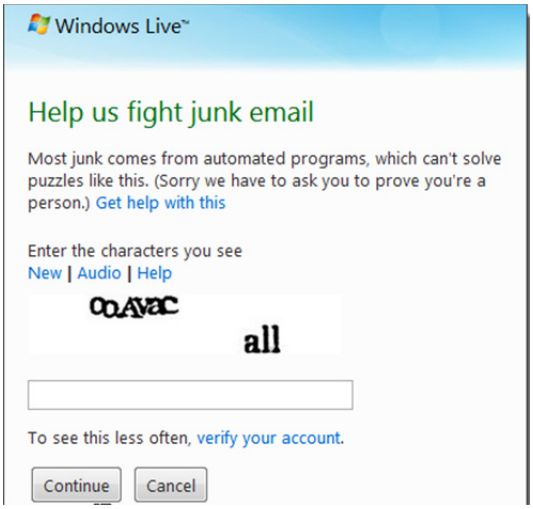

25. Enter your home email address in the To box, clear the **Recipients can edit** check box, and then click **Send**.

26. You may be prompted to complete a security check.



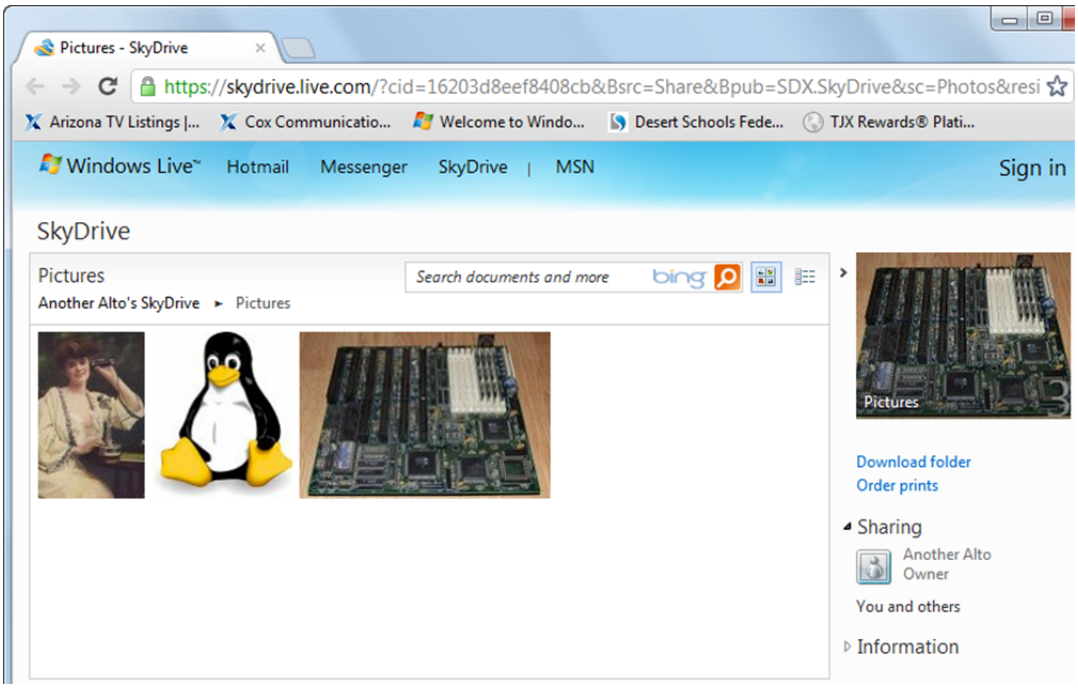

27. Click the **Please complete this security check** link in the message box.

    SkyDrive opens a Hotmail tab in the browser and then asks you to enter the characters you see on the screen. This type of check is called a CAPTCHA – it is used to verify that a human being is sending messages and not an automated program. This type of test helps to reduce spam.

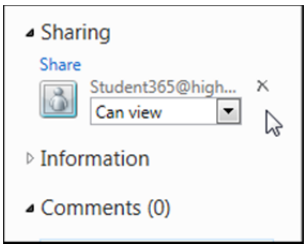



28. Complete the form, then click **Continue**.

29. Close the Hotmail tab and click **Send** again to send your email message. When you open your email, you will receive a message with a link that will allow you to view the *Pictures* folder without signing in to SkyDrive. The figure below shows the email message text. Click the **View photos** link and your browser will open and display the shared SkyDrive folder.




30. The Shared with setting for the *Pictures* folder should now read: **Some people**. The right side of the SkyDrive window should also indicate that the folder is shared and list the people who have permissions. You can stop sharing the folder at any time by clicking the **Delete** button at the right of any of the listed email addresses.




31. Click the **Manage storage** link at the left side of the page to view options for adding more storage.

    Are the fees higher or smaller than you thought they would be? How much storage do you think a home user might require? What about a business user?

32. Click the browser's **Back** button, then click the **Get SkyDrive apps** link to view the available apps for PCs, phones and Macs.
33. Click the browser's **Back** button.
34. In the upper-right corner of the page, click **sign out**.
35. Close your browser.

In this exercise, you explored SkyDrive.

# Understanding Printing Devices

Objective
5.1
5.3

At one time in the not-too-distant past, there was no standard method to connect printers or to instruct various application programs on how to use a printer that was attached to a system. Windows now offers a standard method of connecting to and accessing printers through the creation of a virtual, software-based printer built into the operating system.

To print in Windows, you need a printer and a print device. In the Windows definition, a printer is the set of software components running on the computer that manage the printing process, whereas a print device is the actual physical machine that produces the printed output. That is, the printer is virtual and the print device is the laser or inkjet connected to the computer.

Using this arrangement, software developers write their programs to print to the virtual printer, and Windows converts the applications' data into the correct format for the actual print device being used. Windows also manages the process of communicating with the print device.

This model is advantageous because you need to set up and configure your print device only once (instead of having to set it up for each application you want to use), you can install more than one print device, and printing works the same way whether you are printing to a device attached to your computer or to a print device attached to someone else's computer, or to a network print device.

## Printer Ports

Print devices are connected to computers through ports. A port is a hardware- or software-based interface used to transfer information between a computer and other devices. Hardware ports are physical connections that are visible on the outside of the computer. Software ports are the numbered interfaces in programs that software programs use to exchange information. Modern printers connect directly to a PC through a USB port. Older printers connect directly to a PC through a line printer terminal (LPT) or serial (COM) port. Printers with networking capability are accessed using the static IP address (it is not a good idea to use dynamic IP addresses for printers) assigned to them or by their printer name (which the DHCP server will resolve to the IP address assigned to the printer). Of these two methods, the printer name is more flexible and allows you to change routers and wireless access points without disabling your network printers until the IP addresses are corrected.

## Print Drivers

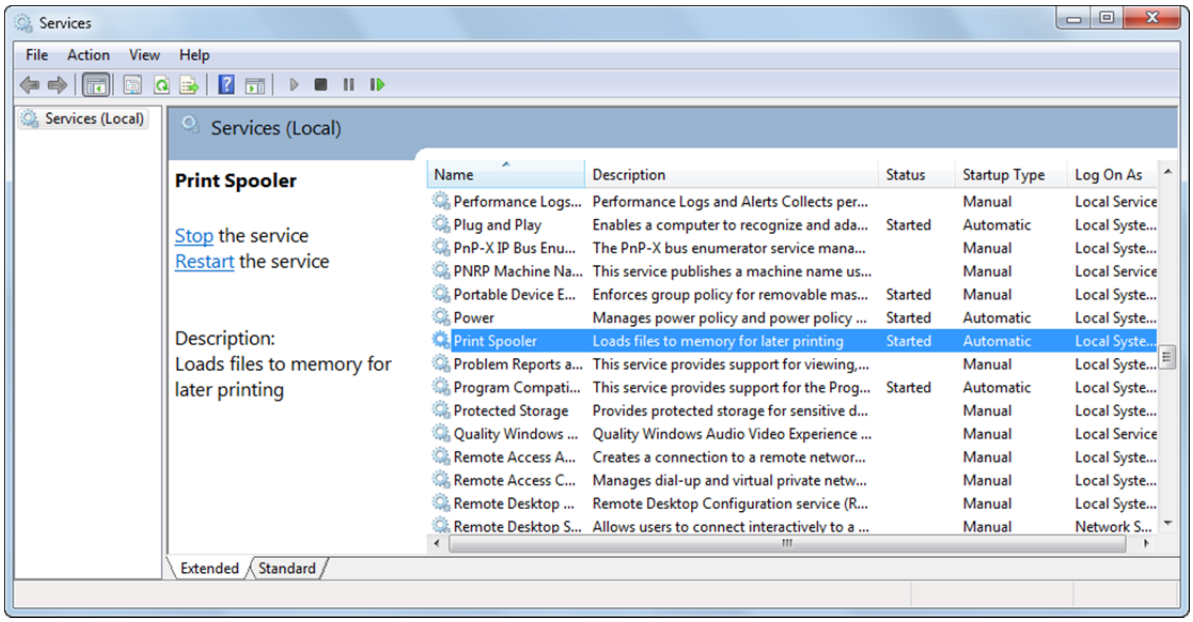
Each print device requires a print driver, which is a program that converts the data to be printed to the form specific to the printer. Windows will automatically install drivers for printers it detects, but in most cases the vendor-supplied installation CD should be used to ensure feature-rich printing.

Many printing issues can be related to an inappropriate print driver. Drivers should be loaded for the appropriate model and can be obtained from the manufacturer’s website. Microsoft Update can also be a resource for driver updates.

## Print Spooler

By default, in Windows, all print jobs go to the print spooler. The print spooler is software that intercepts a print job on its way to the printer and sends it to a folder on the computer where print jobs are stored until they can be printed. Each printer has its own set of jobs retained for it until they may be printed. The print spooler is managed by a service that is displayed as Print Spooler in the Services console.

The Print Spooler is needed because printers operate much slower than the CPU. It was originally developed for the early generation of PC’s when DOS was the operating system. At that time, DOS could only perform one task at a time. Therefore if it concentrated on printing, the user could not do anything until the entire document was printed. Unlike today’s laser printers, the early generation of printers could only print a single character at a time. A document can then take several minutes to completely print. The Print Spooler was developed for DOS to allow the computer to multi-task: i.e. allow users to continue working while the system is printing in the background.

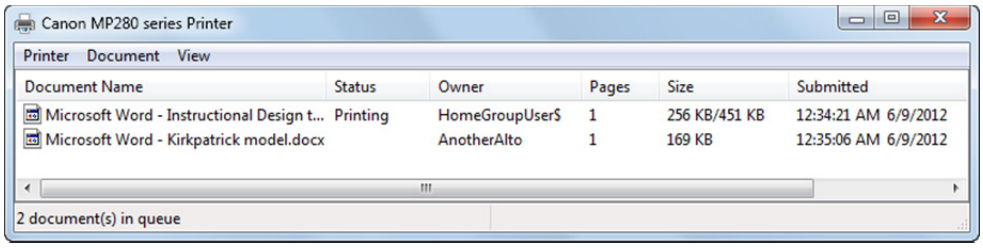



The Print Spooler service manages all print jobs and print queues thereby controlling printing on a Windows system. If you stop the print spooler, the computer will be unable to print.

Restarting the Print Spooler service is a troubleshooting technique when printers stop responding. Restarting the Print Spooler service will clear all the print queues.

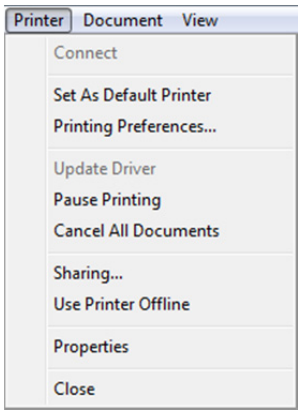
## Print Queue

A print queue is a representation of a print device in Windows. Each printer on a Windows system has a print queue. Opening a print queue displays active print jobs and their status. That is, you can see the job that is currently printing and all the jobs waiting to print.

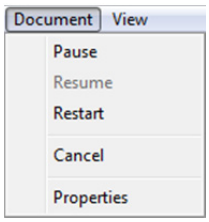



You can access the print queue using the Devices and Printers page of the Control Panel or you can double-click the printer icon in the notification area of the taskbar. This icon displays when you first send a print job to the printer. To access a print queue from the Devices and Printers page, click **Start**, click **Devices and Printers**, click the icon of the printer for which you want to view the print queue, then click the **See what's printing** button in the toolbar.

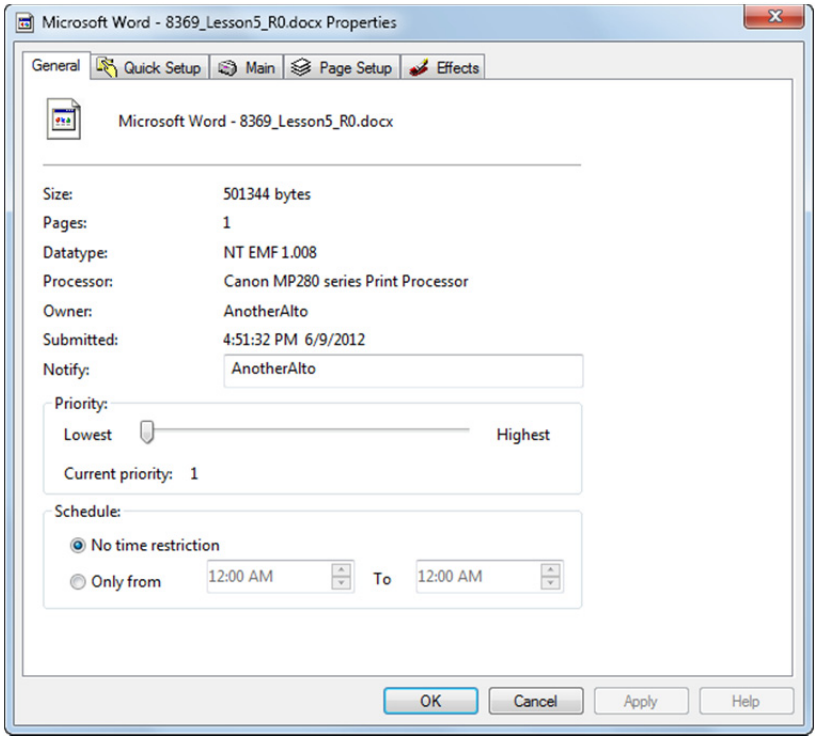
Once you have accessed a print queue, you can pause, restart, or cancel one or more print jobs in the queue. Selections made from the Printer menu affect all jobs in the queue.




Selections made from the Document menu affect the currently selected print job in the print queue.




You can also open the properties page for a print job by selecting the job in the queue and clicking **Properties** in the Document menu, or by right-clicking a print job and selecting **Properties**. From here you can schedule the job, set a priority, and even view the layout and paper/quality settings used when the job was created.




When you increase the priority of a job, you indicate that it should print before other jobs in the queue with a lower priority. If someone has submitted a very large job, you can use the options in the Schedule section to schedule the print job to run after hours so that it does not interfere with print jobs during the work day.

# Using Local versus Network Printers

Local printers are attached directly to your machine. In most cases today, this is with a USB cable. Older printers used parallel cables which connected to parallel printer ports. On modern systems, USB ports have all but replaced parallel ports.

Network printers are printers that are available on the network. Printers can be made available in the following ways:

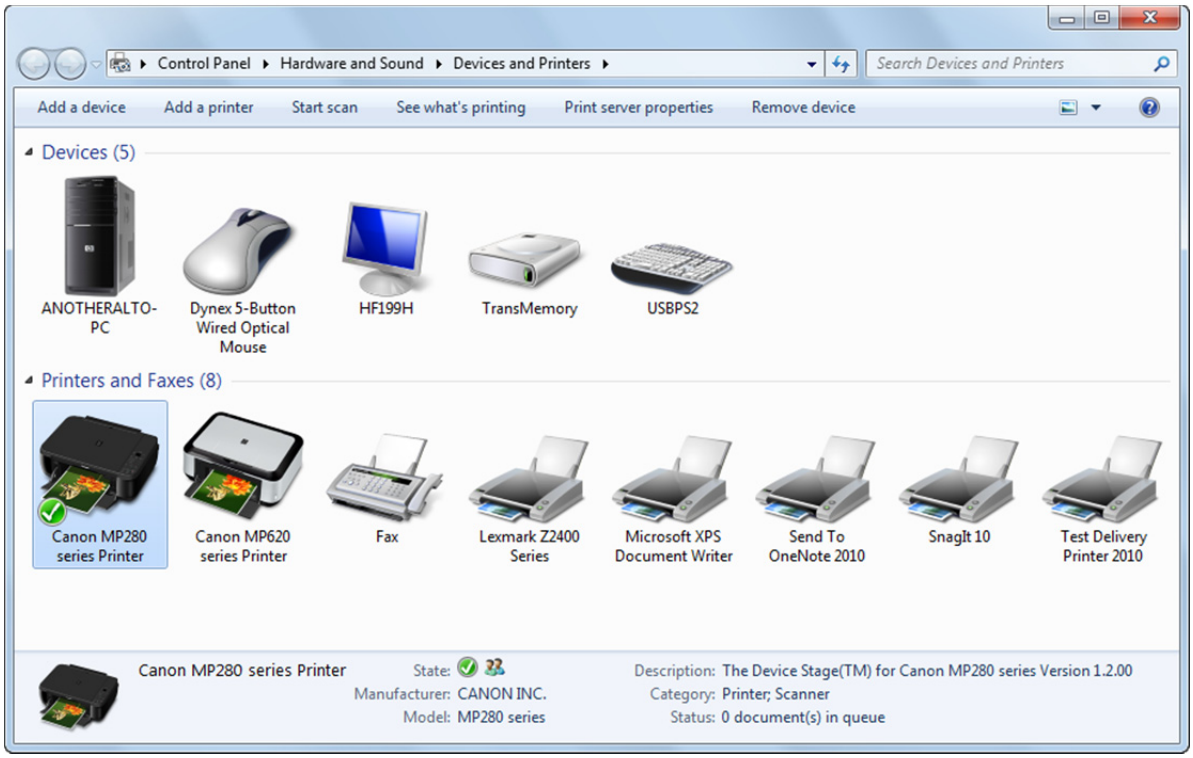
| | |
|---|---|
| **Printer sharing** | The printer is directly connected to another computer as a local printer, and then shared by that computer with the network. As you learned in Lesson 4, when you set sharing properties you can use Windows permissions to control access to the printer. Printer sharing is common in home and small office networks. |
| **Network printers** | These are printers that include Ethernet ports or wireless adapters and are themselves connected directly to the network. They can be accessed either through a print server (this is common in business settings) or through direct access via the network (this is common in home networks). |

**Note:** You can also connect older printers (which do not have internal networking capabilities) to a network print server. The network print server has a built-in connector to the network, and includes one or more parallel or USB ports for connecting to printers.

# Devices and Printers Page

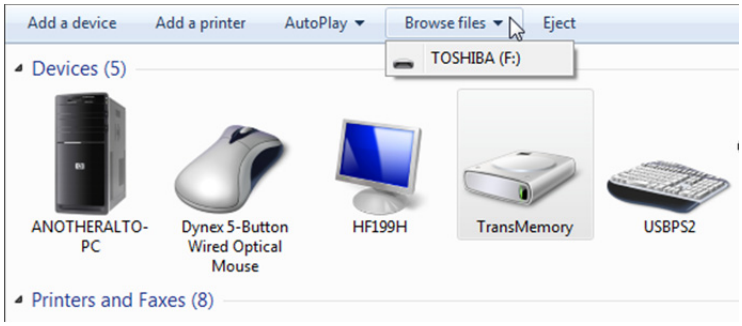
The Devices and Printers page provides an alternate method for adding peripherals. Devices displayed in Devices and Printers are external devices that can be connected or disconnected through a port or network connection.

Open the page by clicking **Start**, then clicking **Devices and Printers**.




Print devices are listed in the Printers and Faxes section. The Fax device allows a user to send a document to the Fax device (as if it were being sent to a printer). It will send the document to a fax modem if one is configured. The Microsoft XPS Document writer allows a user to print a document to an XML Printer Specification (XPS) format. This is referred to as printing to a file. You can also configure your printer to send a print job to a Print to File port, and the print job will be written to a file with a .prn extension.

Note that each type of device has different menu options. In the preceding figure, a printer is selected, and the available menu options relate to printers/scanners. In the following figure, a USB flash drive is selected and the Browse files option is available.



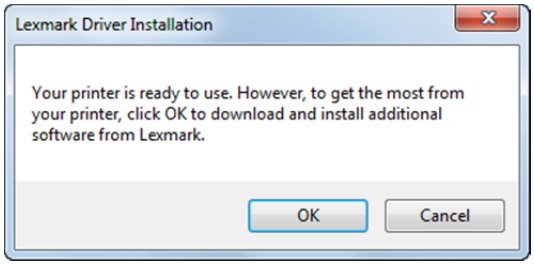

# Connecting and Disconnecting Printers

With many modern printers, you have the option to connect the printer directly to a computer, or to set the printer up for use over a network.

When connecting a printer, you should always read the manufacturer documentation before making any connections. Often printers ship with a "quick start" flyer and a software installation CD. In many cases, you will be directed to run the installation program on the CD before you connect the printer to the system. Installing the manufacturer's drivers first ensures that Windows does not install and use a generic device driver for the printer instead of using the feature-rich drivers supplied by the manufacturer. Once a printer is connected, you should always print a test page to be sure it is functioning properly.

## Connecting a Local Printer

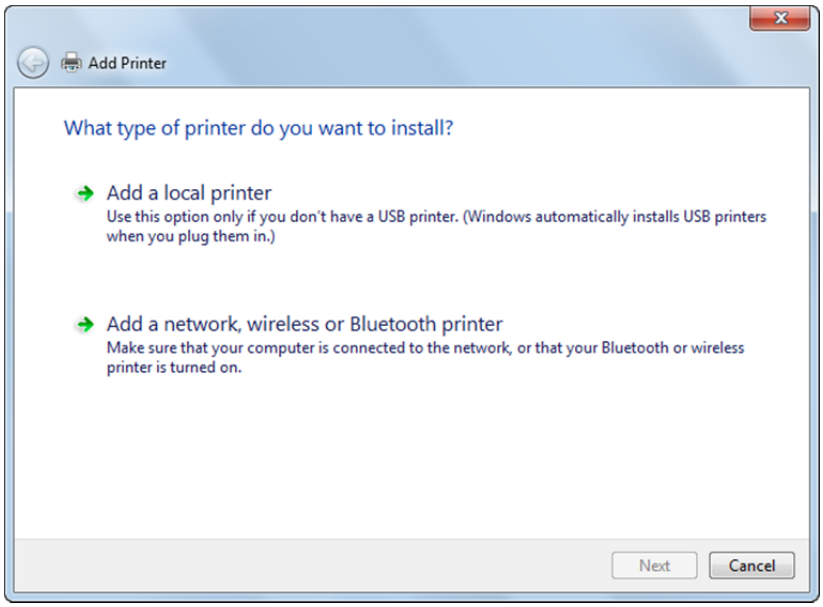
Local printers use direct connections. A direct connection is made by attaching the printer directly to a PC. Direct connections use a parallel printer cable or, more commonly, a USB cable. Windows automatically installs USB printers when you plug them in. You may then be prompted to install additional software from the printer vendor.




Alternatively, you can pre-install the vendor-supplied software and then connect the printer according to the manufacturer's directions, as described in the previous section.

If you are adding an older model printer that connects using a serial or parallel port, follow these steps:

1. Open **Device and Printers**.
2. Click the **Add a printer** button.




3. In the Add Printer wizard, click **Add a local printer**.
4. On the Choose a printer port page, make sure that the **Use an existing port** button and the recommended printer port are selected, then click **Next**.
5. On the Install the printer driver page, select the printer manufacturer and model, and then click **Next**. (If your printer isn't listed, click **Windows Update** and then wait while Windows checks for additional drivers. If none are available and you have the installation CD, click **Have Disk**, and then browse to the folder where the printer driver is located.)
6. Complete the additional steps in the wizard, such as giving the printer a user-friendly name and specifying whether you want to share it, then click **Finish**.

To view a video on adding a printer in Windows, visit http://windows.microsoft.com/en-US/windows7/Install-a-printer.

## Sharing a Printer

If a computer is participating on a network, and that computer has a printer directly attached to it, the user may opt to share the printer with other users on the network by enabling printer sharing. This is different from making a printer a network printer. When a user has enabled print sharing, other computers connect to the printer through the user's computer. Therefore, the computer with the printer attached must be turned on and logged onto the network in order for anyone else to send a document to the printer.

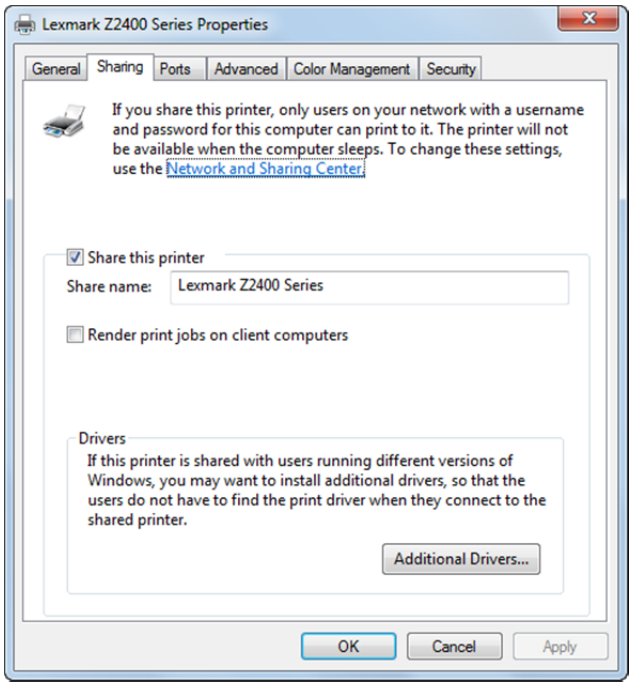
Sharing a printer in Windows 7 is a two-part process. First you must enable file and printer sharing, then you need to share your printer.

To turn on file and printer sharing:

1. Open the **Control Panel** and open the **Network and Sharing Center**.
2. Click the **Change advanced sharing settings** link to access the Advanced sharing settings screen.
3. In the File and printer sharing section, select **Turn on file and printer sharing**, then click **Save changes**.
4. Close the open Control Panel windows.

To share the printer:

1. Click **Start**, then click **Devices and Printers**.
2. Right-click the printer you want to share, and then click **Printer properties**.
3. Click the **Sharing** tab, click the **Share this printer** check box, as shown in the following figure, then click **OK**.



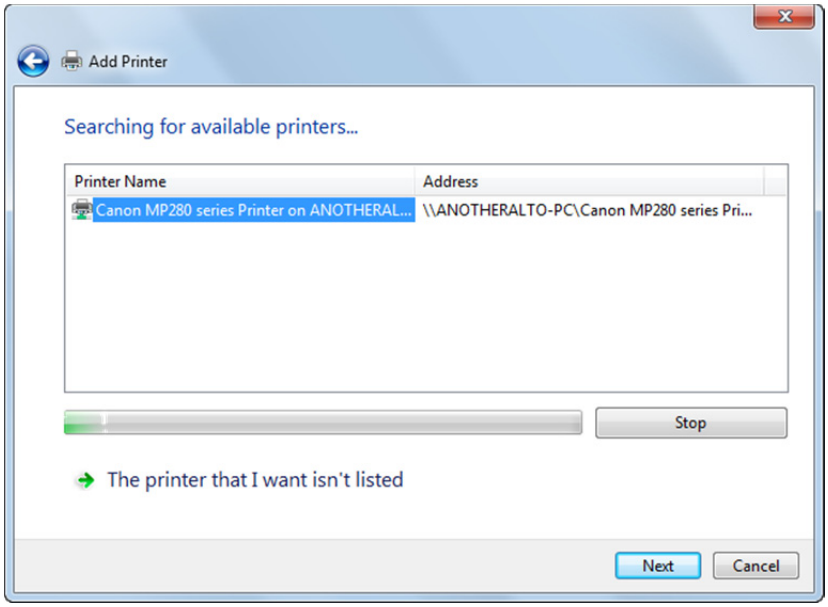

You can clear the Share this printer check box at any time to stop sharing the printer. When you elect to share a printer, you may choose to install additional printer drivers on your system. Doing so makes the drivers available to other users who want to connect to your printer.

To view a video on sharing a printer in Windows, visit http://windows.microsoft.com/en-us/windows7/share-a-printer.

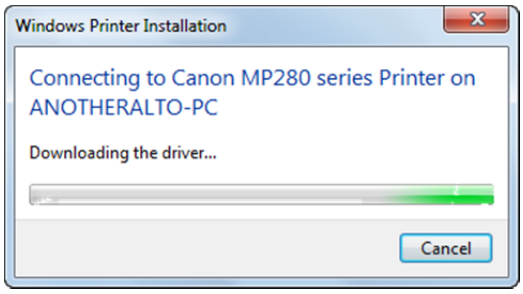
## Connecting to a Shared Printer

To connect to a shared printer:

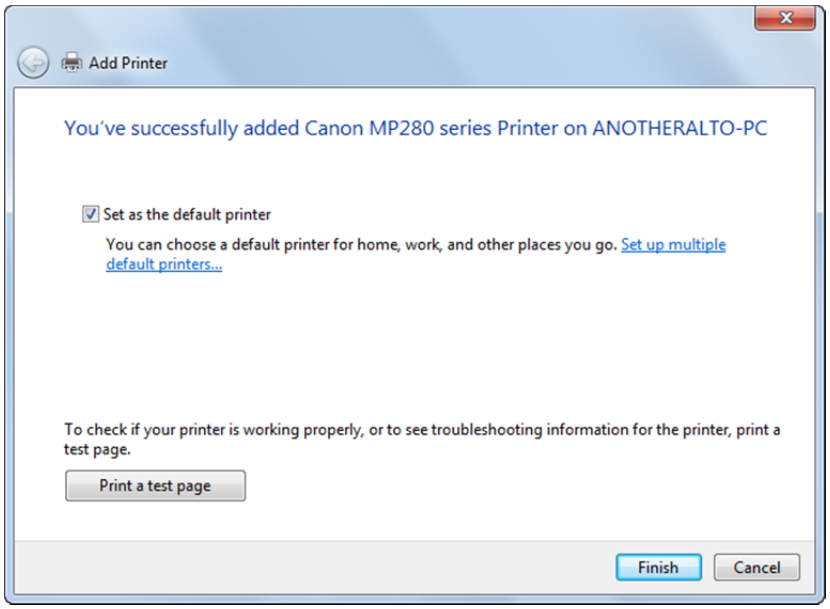
1. Open **Devices and Printers**, then click the **Add a printer** button.
2. Select **Add a network, wireless or Bluetooth printer** in the Add Printer dialog box. Windows will list the printers it finds on the network.




3. Select the printer to which you want to connect, then click **Next**. Windows connects to the printer and installs the required drivers. (If you are asked to install the appropriate drivers, do so and then click **Next**.)




4. When a successful connection is made, Windows displays a success message.
5. Click **Next**. Windows gives you the option to set the newly added printer as the default printer, and gives you the option to print a test page.




6. Click **Finish**.

## Network Printers

Printers can also be set up as network printers. A network printer is different from a shared printer. When you share a printer, other users connect to the shared printer through the computer to which the printer is directly attached. A network printer, on the other hand, is not directly attached to a computer. Rather, the printer is connected to the network.

In order to be set up as a network printer, the print device itself must include an interface for connecting to a network. For example, many printers can be set up as wireless network printers. These connect to a network using wireless networking protocols. Other printers include a network port for wired connectivity. You can plug one end of a network cable into the network port on the printer, and plug the other end into an appropriate device on the network, such as a switch or router.

### Setting Up a Wired Network Printer

When you first set up a printer as a network printer, you must initially connect the printer directly to a PC via a USB cable so you can configure the printer for network use. The PC to which you connect the printer should have an active connection to the network.

You begin by inserting the installation CD into the computer and starting the install program. For printers that include networking options, the installation CDs offer a menu of setup configurations. You would choose an option equivalent to "set up the printer for network use for the first time." Follow the prompts in the installation program and do not connect any cables until instructed to do so.

Generally, the vendor-supplied installation and setup programs will take care of the necessary configurations for you. The procedure usually unfolds in the following sequence: Some initial drivers are loaded onto the PC, and you are then instructed to connect the printer to the PC using the USB cable. The printer and the installation software will communicate with the PC to detect the current network settings. The printer will be given its own network address and the appropriate settings will be configured on the printer. You will be instructed to disconnect the USB cable and connect the printer to a network device using a network cable. You will now be able to access the printer through the network without being directly connected to it.

After the networked printer is configured, you can set up additional PCs or portables to use the printer by installing the appropriate drivers on each machine. Make sure the computer is connected to the network, and then insert the installation CD that came with the printer. Specify that the printer is already set up and that you now want to be able to access it from an additional computer. Usually, the setup program will detect the networked printer on the network and automatically configure the required settings on your computer.

### Setting Up a Wireless Network Printer

To set up a printer as a wireless printer, you must have a functioning wireless access point as part of your network before you begin. (A wireless access point is the networking device that makes wireless networks possible.) You will need to know the name of the wireless network (also called the SSID – pronounced “Sid”), and you will need to know the security passphrase. Most wireless networks use encryption as a security measure. The passphrase is required for wireless devices to gain access.

To set the printer up for the first time, the printer must initially be connected via USB to a computer that is connected to the network. The PC itself does not need a wireless connection to the network; it just needs to be on the same network as the wireless access point.

Insert the installation CD that shipped with the printer, and follow the prompts for setting up a wireless printer for the first time. Connect the USB cable when instructed to do so. Some printers can automatically detect settings for wireless access points; simply follow the instructions that appear on the screen. Some printers will prompt you to supply information on wireless properties such as the SSID and passphrase. Disconnect the USB cable when instructed to do so.

After the printer has been properly configured, you can load the drivers on each computer that wants to access the wireless printer. Usually you insert the installation CD, specify that the printer is already set up, and indicate that you want to configure an additional client to use the wireless printer.

## Disconnecting a Printer

You must be logged on as an administrator to disconnect (remove) a printer. To disconnect a printer:

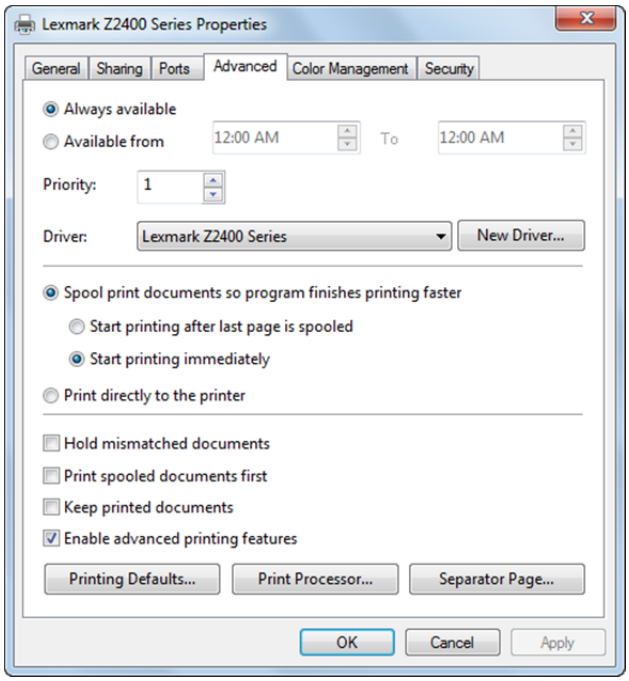
1. Open **Devices and Printers**.
2. Select the printer you want to disconnect.
3. Click the **Remove device** button in the toolbar.
4. Confirm that you want to remove the device by clicking **Yes**.

## Managing Printers

You can use the Devices and Printers page to install, view and manage your printers. Right-click a printer to manage it. Management options include:

| | |
|---|---|
| **See What’s Printing** | Opens the print queue. |
| **Set As Default Printer** | Sets the printer as the one that applications will send print jobs to automatically. Users do not have to select the printer every time they print. |
| **Printing Preferences** | Opens the Printing Preferences dialog box, which you can use to select paper orientation, duplex printing, print quality, etc. |
| **Printer Properties** | Allows you to manage printer properties such as sharing and security. |
| **Remove Device** | Disconnects (removes) the printer. |

The Printer Properties dialog box contains several tabs that you can use to manage features and settings for the selected print device.




The tabs of the Printer Properties dialog box include:

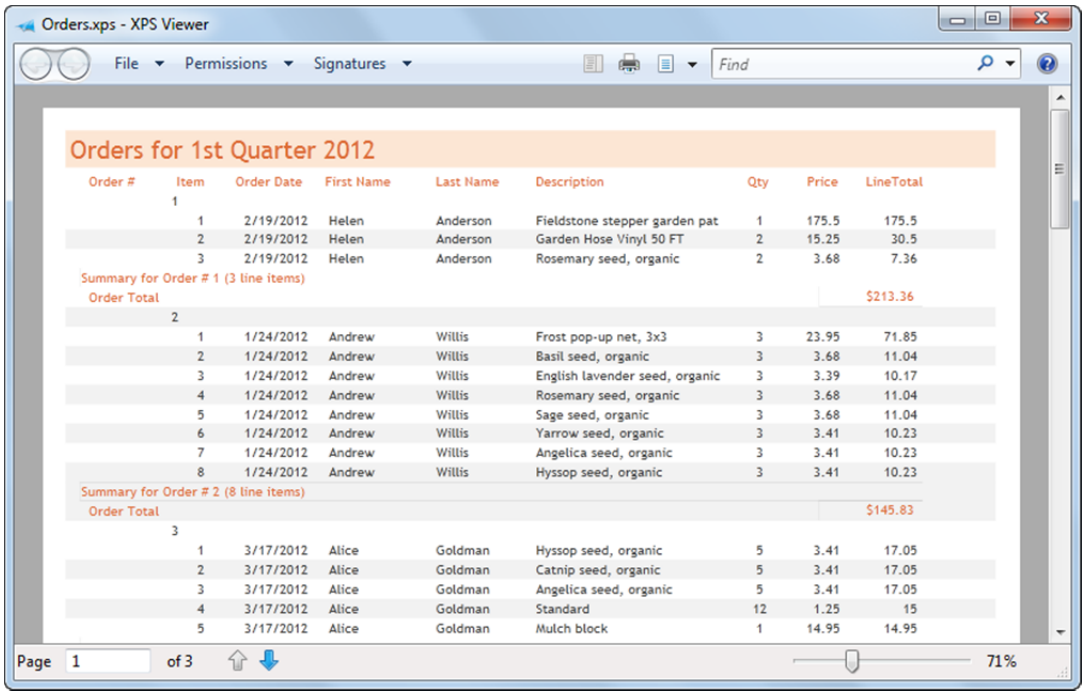
| | |
|---|---|
| **General** | Provides descriptive information about the printer. You can access printer preferences and print test pages from this tab. |
| **Sharing** | Allows you to adjust the sharing settings and specify whether to provide additional drivers to other versions of Windows that may connect to the printer through the share. |
| **Ports** | Defines ports for the computer and specifies which port is being used for printing. Ports can be physical ports, software TCP/IP ports, or File (Print To File) ports. |
| **Advanced** | You can use this tab to select or update drivers and manage spool settings. |
| **Security** | Allows you to grant or deny access to the printer, and define who can manage the printer and its documents and queues. |
| **<Device settings>** | The name of this tab varies with each printer. Generally, this tab provides access to specific features on the printer, such as color management or tray and paper handling, etc. |

## Printing to a File

Many individuals and businesses respect the need to protect natural resources, and more and more organizations are moving toward paperless methods of conducting business. One way to reduce paper consumption is print to files of various types instead of producing printed output on paper.

Windows 7 provides a file type called XPS (XML Paper Specification), which is a Microsoft standard for storing complex documents in XML format. You can print to an XPS file from any application by selecting the Microsoft XPS Document Writer as the printer for the print job.

Although you can create XPS documents using any program that you can print from in Windows, you can view XPS documents only by using the XPS Viewer. The following figure shows a Microsoft Access report printed as an XPS file and opened in the XPS Viewer.




The XPS viewer includes two toolbars. Each toolbar provides options for viewing and managing XPS documents, including:

- Saving a copy of the XPS document to your computer.
- Finding a word or phrase in the read-only XPS document.
- Going to a specific page by typing a page number or by navigating forward and back through the document pages.
- Zooming in or out to make text and pictures easier to read.
- Viewing one or more pages at a time on your screen.
- Digitally signing the XPS document.
- Determining who can access the document and for how long by applying document permissions.

## Printing via the Internet

Internet printing makes it possible for computers running Windows 7 to use printers that are located anywhere in the world. For a Windows 7 machine to print to an internet printer, it must have the Internet Printing Client installed. The client system sends the print job using Hypertext Transfer Protocol (HTTP), which is the same protocol used to browse web pages. Most firewalls are configured to allow HTTP communications through, and in most cases this allows a user to print to a work printer from their home networks without requiring a secure VPN connection.

Following are the server and client components of Internet printing:

| | |
|---|---|
| **Server** | Windows Server 2008 R2 runs the Web Server role, Print Services role, and Internet Printing role. When installed, Internet printing can be enabled on the server. |
| **Client** | A computer running Windows 7 can be used as a client if you install an Internet printer by using a web browser or the Add Printer Wizard. |

The Internet printing process works as follows:

1. A user connects to a printer server across the Internet based on a URL assigned to the device.
2. The print server requires the client to provide authentication information (This ensures that only authorized users can print documents on the print server), and the client responds and is authenticated.
3. The server presents status information to the user, showing which printers are available.

4. The user connects to the printer to which he desires to print. If a driver must be installed, the screens will prompt for driver installation.
5. Once the connection exists, the user can send print jobs to the printer as if it were a local printer.

# Understanding System Devices

Objective 5.4

In general, devices can be classified by their function as input or output devices. Input or output (I/O) devices are used to enable communication between the user and the computer. There are three classifications of I/O devices you can use to:

- Send information to the computer (for example, the keyboard, mouse, trackball, scanner, camera, microphone)
- Display or transmit information from the computer (examples include the monitor, printer and speakers)
- Communicate between computers (for example, modems and network cards)

In simple terms, anything used to enter information into a computer is an input device. Anything that can display information from a computer is an output device. Within this context, video and audio devices are used for capturing (input) and playing (output) media.

Network adapter cards both transmit and receive signals that allow a computer to participate on a network. These devices perform both input and output functions.

## Using Video Devices

Video cameras and web cameras are video input devices.

Video cameras are attached to the PC through an external port (e.g., USB or FireWire), and web cameras can either be attached to an external port or built into the screen area of a laptop.

Web cameras (or webcams) are specialized cameras that are designed to record live video and transmit it across a network or the Internet. A webcam must be connected to either a computer or a network. If connected to a computer, the connection is usually USB. If connected to a network, the connection is generally Ethernet or a wireless connection.

Video input devices require drivers and often require special (vendor-supplied) software as well. While drivers enable these cameras to function, the additional software provides practical use for the devices.

The most popular use for webcams is for making video phone calls. Many webcams include built-in microphones and most include software for video email, video capture, videoconferencing, and still-image capture. Many people use their webcams to make video calls using an instant messaging service such as Skype, Windows Live Messenger or Yahoo Messenger.

## Using Audio Devices

Audio devices capture and play sound. Most of these devices can connect to a PC through ports on the sound card or through USB or wireless connections.

Microphones can be used for audio input. These can include:

- Internal microphones on laptops
- Analog microphones connected to the sound card through the Mic 3.5mm audio jack
- Digital microphones connected through USB ports

Like video input devices, audio input devices require drivers and often times require special software as well.

Headphones, headsets and speakers are audio output devices. Headphones can connect to a computer through a dedicated headphone jack or a Line-Out jack on the sound card. Some CD-ROM drives also include a headphone jack. Headsets usually connect to a computer through a USB or wireless (Bluetooth) connection.

Sound cards are designed to work with external speakers on a desktop system and special built-in speakers on a laptop. External speakers require a power source. Although some small USB-powered computer speakers are available, speakers that produce high-quality sound must be plugged in to an electrical outlet. Speakers are connected to a computer through the Line-out 3.5mm audio jack on the sound card. Sound cards with separate jacks for rear, mid and center surround sound allow you to fine tune the sound produced by your system.

While drivers are required for audio output devices, special software is generally not required.

# Using Infrared Input Devices

Infrared (IR) transmission is a form of free-space transmission that uses low-frequency infrared (IR) light to transmit signals. Infrared is a type of light that is not visible to the human eye.

IR can be easily and inexpensively used to allow two devices to communicate with each other. The transmission speed is fast because light travels at 186,000 miles per second. However, IR transmissions have a very limited range (no more than 15 feet) and require a clear path between the transmitter and the receiver. Walls and other obstructions will block these transmissions, and bright light (such as sunlight) will degrade them. Also, IR communications are limited to sending or receiving one byte of data at a time. Compounding this problem is the fact that the IR device can only send or receive at any one time, and if it tries to switch from sending to receiving too quickly it will actually receive a reflection of the same signal it had just sent. Therefore, although the speed of transmission is fast, the total amount of data that can be exchanged between two IR devices is very low because each must wait before sending the next byte of data. Instead, IR communication works best when it is used to transmit in one direction only.

Due to these limitations, successful use of infrared technology has been limited to a small number of input devices such as mice, keyboards, and remote controls for media players.

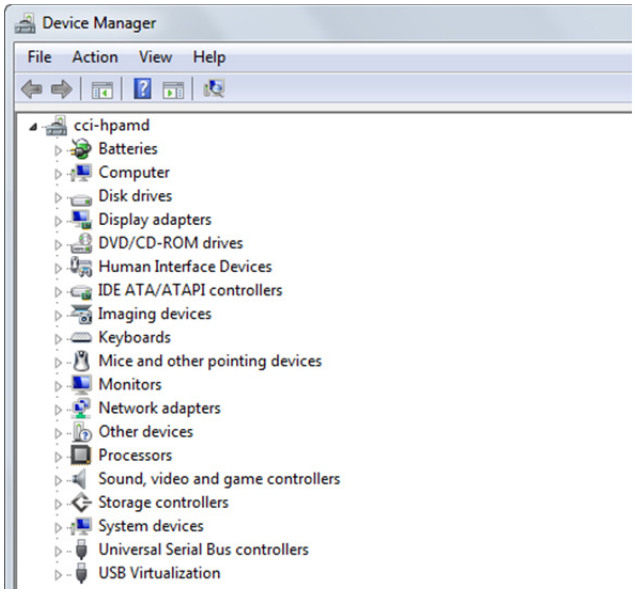
As with other devices, the proper device drivers must be acquired and installed.

# Using the Windows Device Manager

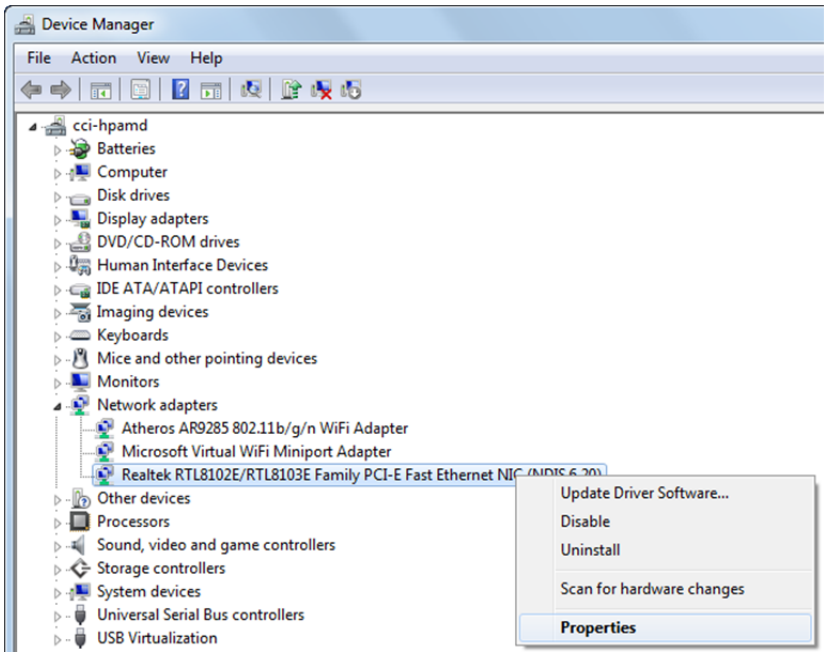
The Windows Device Manager is a Microsoft Management Console (MMC) snap-in tool that provides a graphical view of the hardware that is installed on your computer. While you use the Devices and Printers page to manage external devices that can be connected or disconnected through a port or network connection, you use the Device Manager to manage devices and components that are installed internally.

As you have learned, all devices communicate with Windows through device drivers. You can use the device manager to install and update the drivers for your hardware devices, modify hardware settings for those devices, and troubleshoot problems.

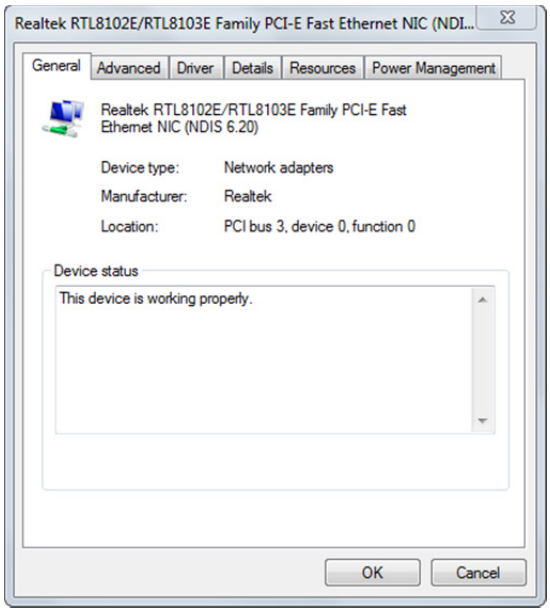
To open the Device Manager, open the Control Panel in Large or Small icons view, then click the **Device Manager** link. The Device Manager is shown in the following figure.




You can view a listing of the devices installed on a system, view device driver details, find updated drivers and view or change the current status (enabled or disabled) of each device. Devices are arranged in categories, such as Display adapters, Keyboards, Network adapters, etc. To expand a category, click the arrow to the left of the category name.

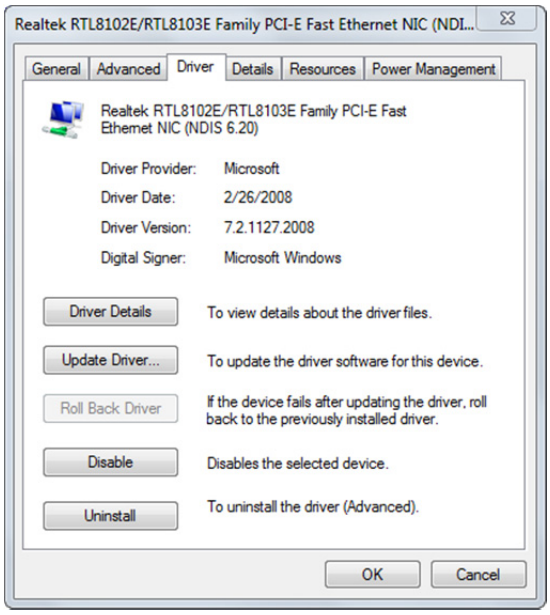



By right-clicking on a device in the Device Manager window, and selecting **Properties**, you open the Properties dialog box for the selected device.




The tabs in the Properties dialog box will vary depending on the type of device selected. The tabs in the preceding figure will indicate if the device is working properly, show advanced settings for the device, supply details about the device driver, supply details about the device itself, show which resources are allocated to the device, and show the available power management options.

Click the **Driver** tab to view information about the driver provider, date and version. The Driver tab also includes buttons for viewing details about the driver files, updating drivers automatically, rolling back a driver, disabling the device and uninstalling the device.




**Note:** You can also right-click a device in the Device Manager window and select **Update Driver Software**. Selecting this option launches the Update Driver Software wizard. The wizard allows you to have Windows search your computer and the Internet for updated drivers automatically, or to allow you to browse your computer for driver files that you have downloaded or copied to a storage location. After you browse to the driver files, you can install them manually.

## Rolling Back a Driver

After you update a driver, the **Roll Back Driver** button becomes available in the Properties dialog box. You may want to roll back a driver to its previous version if the device for which you updated the driver begins to malfunction. To roll back a driver for a device, locate the device in the Device Manager, right-click the device and select **Properties**, click the **Driver** tab of the Properties dialog box, click the **Roll Back Driver** button and follow the instructions in the wizard to replace the updated driver with the previous version.

## Disabling Drivers

If you suspect that a device driver is interfering with the operation of a system, you can use the Device Manager to temporarily disable the driver and the device to see if the problem is resolved. To disable a device, open the Device Manager, expand the category, right-click the device in question and select **Disable** from the shortcut menu. Click **Yes** to confirm that you want to disable the device. When a device is disabled, it displays a small down-facing arrow in the icon to the left of the device name. To enable a device, right-click the disabled device and select **Enable** from the shortcut menu.

When you disable a device in the device manager, you make it nonfunctional. For example, if you disable a wireless network card, you cannot use the device until you enable it once again. Disabling a device frees the resources that were allocated to the device.

# Exercise 5-2: Using the Windows Device Manager


In this exercise, you will use the Windows Device Manager. Note that you must be logged in as an administrator to see all options available.

1. Click the **Start** button, type: `Device Manager` in the Search box, then press ENTER.
2. In the menu bar at the top of the window, click **View**, then select **Resources by type** to change the way devices are listed.
3. Expand **Input/output (IO)** to view I/O addresses.
4. In the menu bar at the top of the window, click **View**, then select **Devices by type** to change back to the default arrangement.
5. Click **View**, and then select **Show hidden devices**. Are any additional devices visible? If so, what are they?

   _____

6. Click **View**, and then select **Show hidden devices** again to toggle the setting off.

7. Expand the Network adapters, and then list the adapters that are installed.

   a. _____

   b. _____

   c. _____

8. Right-click a network adapter (preferably an Ethernet adapter if one is installed) and select **Properties**. Who is the manufacturer listed on the General tab?

   _____

9. Click the **Advanced** tab to view a list of property settings for the device. If they are available, record the values for the following properties:

   Priority & VLAN _____

   Speed & Duplex _____

   Note these properties may be named a little differently for your adapter (depending on the manufacturer); however the name(s) will be similar.

10. If the Speed & Duplex property is available, display the drop-down list and note the variety of choices. When this property is set to Auto Negotiation, the network card will adjust to the speed and communication flow used by the device with which it is in communication.

11. Click the Driver tab and record the following information:

    Driver Provider _____

    Driver Date _____

    Driver Version _____

    Digital Signer _____

12. Is the Roll Back Driver option available? What does this indicate?

    _____

13. Click **Cancel** to exit the Properties dialog box.

14. Right-click the same adapter, select **Uninstall** and click **OK** to acknowledge the warning. Do NOT select the Delete the driver software for this device option.

15. Try to access the Internet. Are you able to?

16. Did the appearance of the network icon in the notification area of the taskbar change? If so, in what way?

    _____

17. Return to the Device Manager and in the Menu bar click **Action**, then select **Scan for hardware changes**.

18. Did Windows find the network adapter and install the appropriate drivers for it?

19. Can you access the Internet now?

20. Close all open windows and dialog boxes.

In this exercise, you used the Device Manager to view device properties, uninstall a device and then scan for hardware changes.

# Lesson Summary

In this lesson, you learned how to manage devices connected to your computer. You are now able to:

- ☑ Explain the purpose and function of device drivers.
- ☑ Describe how compatibility issues between drivers and the operating system can affect the system.
- ☑ Describe how and when to update device drivers.
- ☑ Explain system resources and resource allocation.
- ☑ Explain the features and function of Plug-and-Play technology.
- ☑ Explain when to install third-party software for devices.
- ☑ Describe storage device interfaces.
- ☑ Describe the function of RAID.
- ☑ Describe basic, dynamic and virtual hard disks.
- ☑ Describe the process of using cloud storage.
- ☑ Describe printer ports, printer drivers, the Print Spooler, and the Print queue.
- ☑ Compare and contrast local printers and network printers.
- ☑ Use the Devices and Printers page
- ☑ Explain how to connect and share a local printer.
- ☑ Explain how to connect to a shared printer.
- ☑ Explain how to disconnect printers.
- ☑ Describe how to manage printers.
- ☑ Explain the purpose and function of the Microsoft XPS Document Writer.
- ☑ Describe how printing over the Internet works.
- ☑ Explain video, audio, and infrared devices.
- ☑ Describe how to use Windows Device Manager.

**MMM**
Go online for Additional Review and Case Scenarios

# Review Questions

1. Mikayla wants to add a printer to her PC. Where should she go to add the printer?
   a. The Devices and Printers page
   b. The Windows Device Manager
   c. The Computer Management console
   d. The Disk Management snap-in

2. What is the minimum number of disks required for RAID 5?
   a. Two.
   b. Three.
   c. Four.
   d. Five.

3. Which of the following is required for using SkyDrive?
   a. 4 GB RAM
   b. A 2.8 GHz processor
   c. A Windows Live ID
   d. SkyDrive 3.2 device drivers

4. By default, where do all print jobs in Windows go?
   a. To the COM1 port.
   b. To the Microsoft XPS Document Writer
   c. To the Print Spooler.
   d. To the Windows Device Manager.

5. Print jobs can be sent across the Internet using which protocol?
   a. Hypertext Markup Language (HTML)
   b. XML Paper Specification (XPS)
   c. Internet Print Protocol (IPP)
   d. Hypertext Transfer Protocol (HTTP)

# Lesson 6: Maintaining Your System

## Lesson Objectives

In this lesson, you will learn about various tools and methods for maintaining a Windows 7 system. By the completion of this lesson, you will be able to:

- ☐ Identify various types of malware.
- ☐ Identify security risks other than malware.
- ☐ Explain how malware affects the Windows Registry.
- ☐ Explain the use of firewalls.
- ☐ Describe the function and purpose of antispyware software.
- ☐ Describe the function and purpose of antivirus software.
- ☐ Describe how to avoid malware infection.
- ☐ Understand the function of the Windows Action Center.
- ☐ Explain and use the Malicious Software Removal Tool.
- ☐ Describe and use Windows Defender.
- ☐ Describe the function of Microsoft Security Essentials.
- ☐ Describe the function of Microsoft Forefront Endpoint Protection.
- ☐ Explain Windows Backup and Restore.
- ☐ Describe the function of system images, restore points and previous versions.
- ☐ Explain Advanced Boot Options, including Safe Mode and Last Known Good Configuration.
- ☐ Describe Microsoft update types.
- ☐ Explain how to use Windows Updates.
- ☐ Explain and use Windows system maintenance tools, including Defrag and Disk Cleanup.
- ☐ Explain how to use the Task Scheduler.
- ☐ Describe the purpose and function of the System Information tool.

### Exam Objectives

3.3 Remove malicious software
6.1 Understand backup and recovery methods
6.2 Understand maintenance tools
6.3 Understand update

## The Need for Security

As soon as you connect a computer to a network, you expose that system, and the information stored on it, to the potential risks associated with networking. The information stored on a networked computer can, in theory, be accessed by any computer connected to the network. If the network provides Internet access, the risk increases. Any person who attempts to gain unauthorized access to a computer system is known as a *hacker*. Hackers employ many different methods to obtain what they want.

To combat these risks, IT professionals design and implement specific policies related to security. The rules and procedures defined in the security policy should address three principles: confidentiality, integrity and availability.

| | |
|---|---|
| **Confidentiality** | The ability to keep data secret and viewable only by authorized parties. To protect confidentiality, a security policy must ensure that information can flow across the network without being intercepted. Messages are encrypted before being sent across the network. |
| **Integrity** | Verifying that data has not been illicitly changed or tampered with. Digital certificates and digital signatures are used to verify data integrity. Policies designed to protect data integrity also include rules for backup procedures. |
| **Availability** | Ensuring that authorized parties can readily access information. To ensure availability, networks are designed with redundant connections to eliminate single points of failure; backup systems use hot-swappable drives and networks are monitored for any suspicious activity which may preclude an attack. |

Furthermore, security policies must be in place to keep enterprise assets operating at peak efficiency, to ensure that they are free from malware, and to ensure that data is regularly backed up to protect against catastrophic loss.

As you read about risks and ways to combat them you should notice that user education and cooperation are vital to the success of IT security policies.

# Identifying Risks

Whether you are an IT professional, or an avid user, you should be aware of potential risks you face when you connect to a network or to the Internet.

## Malware (Malicious Software)

*Malware*, or malicious software, refers to programs or files whose specific intent is to harm computer systems. Malware is an electronic form of vandalism that can have global implications. IT professionals must be aware of malware to be able to detect and remove malicious code before it harms systems and networks. Malware includes computer viruses, worms and Trojan horses.

### Viruses

A *virus* is a malicious program designed to damage computer systems. Specifically, a virus is a program that takes control of system operations, and damages or destroys data. Viruses are loaded onto your computer without your knowledge and run without your consent. All computer viruses are human made and are often designed to spread to other computer users through networks or email address books.

Viruses can be transferred via email attachments, program or file downloads, and by using infected disks, CDs, or flash drives. If you pass an infected drive to a co-worker, that co-worker's system can also be infected. Similarly, a colleague might inadvertently send you an email attachment infected by a macro virus. If you attempt to open or print the file, the virus will engage. Email attachments have become the most effective way to spread viruses.

A virus can:

- Display harmless messages on the screen.
- Use all available memory, thereby slowing or halting all other processes.
- Corrupt or destroy data files.
- Erase the contents of an entire hard disk.

### Worms

A *worm* is a self-replicating program that consumes system and network resources. The difference between a worm and a virus is that a worm automatically spreads from one computer to another, whereas a virus requires some form of action; for example a user must pass an infected disk to someone else, or must forward an infected email message.

A worm can reside in active memory and replicate on the network. Worms can spread to all computers connected to a network and are commonly spread over the Internet via email attachments.

## Trojan Horses

A *Trojan horse* is a program designed to allow a hacker remote access to a target computer system. The code for a Trojan horse is hidden inside seemingly harmless applications, such as games. Trojan horses are installed on the target system when the user runs the infected application. Unlike worms and viruses, Trojan horses do not replicate themselves or copy themselves to other files and disks.

Once installed on the target system, the Trojan horse can allow a hacker to take control of the target system, steal information, install other software (including malware), download or upload files, or crash the system.

Trojan horses can be accidentally installed through software downloads (e.g., a Trojan horse is included as part of a software application downloaded from a network), through websites containing active content (e.g., a Trojan horse in the form of an ActiveX control), or through an email attachment.

## Spyware / Adware

*Spyware* is a software application that is secretly placed on a user's system and gathers personal or private information without the user's consent or knowledge. *Adware* is a software application that automatically displays or downloads advertisements.

Many Internet-based applications contain spyware. Companies with both good and bad reputations have included spyware code in their software. Spyware can also be placed on a user's system by a virus or by an application downloaded from the Internet.

Once installed, spyware monitors the user's activity on the Internet and conveys the information to the spyware originator. The originator can then gather website usage, email and even password information from the user, then use it for advertising purposes or malicious activities.

Spyware can consume memory resources and bandwidth. Spyware has the ability to:

- Scan files on hard drives.
- Read cookies.
- Monitor keystrokes.
- Install other spyware applications.
- Change the default home page in web browsers.
- Automatically send information to the spyware developer.

Although cookies themselves are not dangerous, they can be used to store user names and passwords if you click "Yes" when your browser asks you if you want to store this information. Cookies also track browser activities, such as sites you visit and options you select.

In a normal Internet transaction, cookies are read only by the server that placed them on your system; however, a hacker who gains physical access to your system or successfully installs spyware can steal your cookies, and with them, any stored user names and passwords.

You can download and install freeware spyware/adware applications, or you can use Windows Defender to monitor your system for spyware. Antispyware applications are discussed later in this lesson.

## Bots / Zombies

A "bot" is a type of malware which allows an attacker to gain control over an affected computer for the purposes of fraudulent use, such as sending spam, hosting phishing websites or attaching websites. Computers that are infected with a bot are generally referred to as zombies because their legitimate users have no knowledge that the systems are being used for illicit purposes.

Bot programs run in the background undetected by legitimate users. The best way to protect against bot infection is to run antivirus/antispyware software and to keep the operating system up to date.

# Other Risks

Most of the risks described in this section are associated with taking advantage of uninformed users. Consider these risks when determining the type of user account to assign to employees.

## Social Engineering

Social engineering is the practice of tricking employees into giving out passwords or other types of access information. Social engineers pose as fellow employees, technical consultants or cleaning staff, in order to gain the trust of real employees.

Social engineers count on people's desire to be helpful. For example, a social engineer may wait near a secured door that requires a smartcard for access and wait until a legitimate employee is about to enter. The social engineer could then approach the door carrying an armload of boxes. Out of courtesy, the real employee may then hold the door open so the social engineer can enter.

Social engineers also attempt to imitate a legitimate user by confusing a switchboard operator or a security guard. In several instances, a social engineer has actually called a company, posing as the systems manager. After explaining that he had accidentally locked himself out of the computer, he convinced someone in the company to change administrative access according to his instructions. All the social engineer then had to do was log on to the machine, and he had full administrative access.

Typical targets of the social engineering strategy include anyone who has access to information about systems they do not use, including secretaries, janitors, some administrators and even security staff.

### Reducing the Risk of Social Engineering

The best way to guard against becoming a victim of social engineering is to recognize common social engineering practices. Following is a brief list of social engineering strategies:

- Posing as a technician and using that implied authority to cause employees to divulge information, to make configuration changes to servers, or to obtain sensitive information.
- Confusing or intimidating an employee or guard into allowing physical access to a building.
- Sending official-looking email messages to all employees with instructions that cause them to reveal sensitive information.

To reduce the risk of social engineering, consider the following strategies:

- Educate all employees.
- To protect a truly sensitive resource, make sure the security policy requires that a certain number of employees must first give approval to gain access to that resource. This way, no single employee can be tricked into allowing illicit access to an essential resource.

## Phishing

Phishing is the process of trying to gather sensitive information such as a password, or credit card details from an unsuspecting victim by pretending to be a trustworthy entity. Typically, a phisher sends a legitimate-looking email message that directs the recipient to visit a fraudulent website that looks identical to a legitimate site. Victims are then asked to update personal information (such as password, credit card or bank account numbers) on the fraudulent website. The phisher can then use the captured information for malicious purposes, including identity theft. A sample email phishing scam is shown:


HSBC The world's local bank

Dear HSBC account holder,

In order to make your online experience even more secure we have introduced a new security feature that allows us to detect unusual activity on your online account.

Please Log On Here To Update Your Account Now!!!

Please note that accounts not renewed within **24hrs** of suspension are subject to termination.

*Collette Nugent*
Head of Customer Communications
**HSBC Internet Banking**

To combat phishing:

- Enable the antiphishing features in your browsers.
- Check an unknown site manually. (In Internet Explorer, click **Tools**, point to **Safety**, then click **Check This Website**.)
- Avoid clicking links in email messages. If a message appears to have come from a bank, credit card company or government agency, call the organization directly to discuss the email message. Often you will be informing the genuine company that a fraud scheme is in place so they can send appropriate notices to their clients.
- Before logging in to a secure site, check the Address bar to be sure the address starts with the legitimate site name.

## Identity Fraud

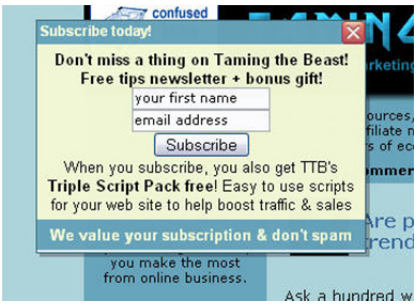
When a hacker obtains a legitimate user name and password, he can log on to a network. The level of access the hacker gains depends upon the rights and privileges associated with the stolen account. However, most network administrators configure the network to track user logons. If a hacker logs on using your account, and manages to damage the network, the electronic trail may lead to you. If you suspect that your account has been compromised, contact the network administrator immediately so you can change your user name and password.

Similarly, most smartcard readers on doors to secured areas maintain logs. The logs indicate who entered through the door and when. If a hacker enters a secured area using your stolen card and damages the network, the logs may point to you. If you misplace your access card, notify the proper person immediately.

## Pop-ups

A pop-up is a small window that suddenly appears and usually displays advertising content. While the pop-up window itself is not dangerous, pop-ups can include links to malware or may prompt users to install software which might contain a virus or spyware.

Proceed with caution when granting a pop-up permission to install software. Keep in mind, however, that inexperienced users may not be aware of the dangers of indiscriminately clicking links in pop-up windows. Configuring a browser to suppress pop-ups is often the safest choice.




## Indiscriminate Link-clicking and Anonymous Downloads

While most users are fairly well educated on the dangers of clicking links in email messages, many do not give a second thought to clicking links in pop-up windows, instant messaging windows or chat rooms. These links may install spyware or viruses or applications that contain Trojan horses. Although antivirus applications and resident scanner programs can check all incoming email, they cannot monitor links in these interactive windows.

Users may also browse to *poisoned websites*. Poisoned websites contain malicious content designed to harm computers. Simply visiting a poisoned website can infect or destroy the data stored on a system.

Poisoned websites may also contain *drive-by downloads*, which download Trojan horses, spyware, viruses or other malware without the user's knowledge or consent. The site may display a link or pop-up window that, when clicked, initiates the drive-by download with no indication to the user of having begun any download process.

Several antivirus applications include "safe searching" or "safe surfing" options. With these options enabled, the applications can report possible dangerous web pages in the search results and block object downloads that may harm your system. AVG (http://free.avg.com) and the latest versions of spyware and virus removal products from Norton (www.symantec.com) and McAfee (www.mcafee.com) are examples of antivirus products that include safe searching/surfing options you can use to protect your system from poisoned web pages.

## Accidental Mis-configuration

Sometimes holes are accidentally created in otherwise secure networks through mis-configurations. Mis-configurations include:

- Accounts with easily-guessed passwords.
- Corporate web browsers configured to allow Java and other active content.
- Storing sensitive data on servers that are accessed from the unsecured public network. For example, you should not store confidential employee records on a web or FTP server.
- Mis-configured network equipment, such as firewalls that do not sufficiently screen incoming or outgoing traffic.

# Malware and the Windows Registry

Objective 3.3

The Windows Registry is a central, hierarchical database in Windows used to store information necessary to configure the system for one or more users, applications and hardware devices. The Registry contains information that Windows references during operation, such as user profiles, installed applications and the types of documents each can create, settings for folders and application icons, installed hardware and which ports are used for communication.

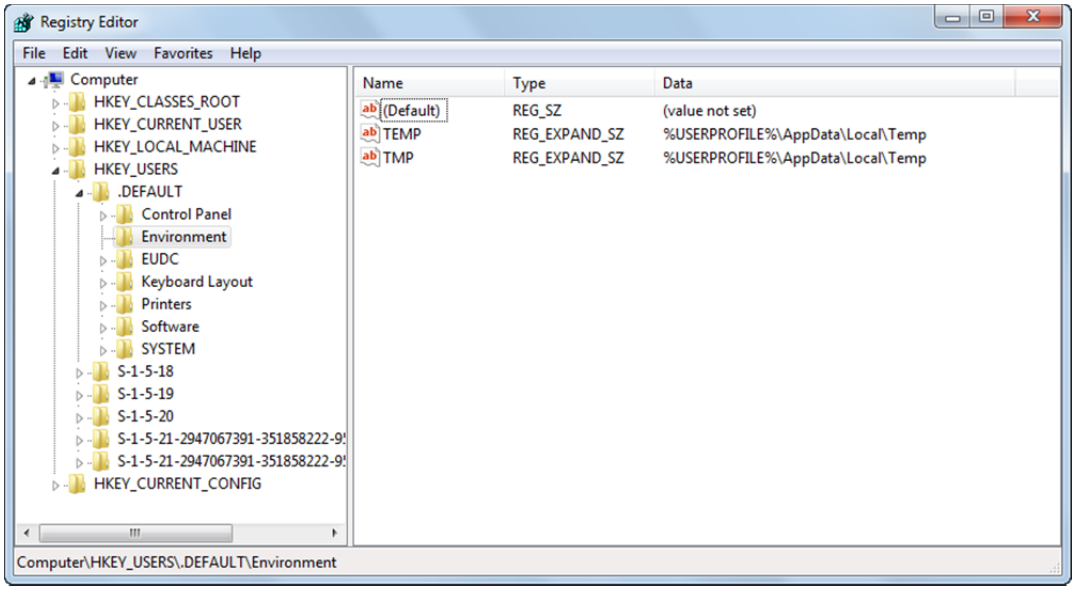
Malware attempts to exploit certain sections of the Registry. In most cases, malware is installed and configured so that it starts each time your system starts. The Registry includes locations that contain applications and services that should start automatically when the system starts.

To view and/or modify entries in the Windows Registry, open the Registry Editor application. Click the **Start** button, type: `regedit` in the search box, press ENTER, and click **Yes** in the User Account Control.

A hive in the Windows Registry is the name given to a major section of the registry. Each hive contains registry keys, registry subkeys and registry values. All keys that are considered hives begin with HKEY and are at the top of the registry hierarchy. A key in the Windows Registry can be thought of as a file folder. A key that resides within another key is called a subkey. Registry keys may contain additional subkeys and registry values.

When you view the Windows Registry in the Registry Editor, the hives and keys appear as folders on the left side of the window.

A value in the Windows Registry contains specific instructions. In the Registry Editor, values appear on the right side of the window. The following figure shows the Windows Registry open in the Registry Editor.




Malware often adds or modifies registry entries. The following registry locations are affected by malware:

- **\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** – this location contains folders (Run, RunOnce, RunServices, and RunServicesOnce) that are part of the autostart registries. The applications in these folders are what Windows executes immediately after a system is started.
- **\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion** – this location also contains autostart registry folders Run, RunOnce, RunServices, and RunServicesOnce.
- **\HKEY_CLASSES_ROOT** - this location contains entries that determine which applications or programs to run for certain file extensions. Malware applications can modify the associations of commonly used file extensions and launch more malware when the user or a program tries to open a particular file type.

At times, antimalware applications may not be able to clean or remove infected files, and you may have to remove illegitimate registry entries in order to clean the system. Always follow the instructions carefully, and always back up registry entries before modifying or deleting them.

You can back up a registry entry by opening the Registry in the Registry Editor, right-clicking the entry and selecting Export. Save the exported entry to a file. After creating a backup, you can delete or modify the registry key. If you find that what you deleted is a normal entry and not a malware entry, you can restore it from the backup.

# Mitigating Risks

Firewalls help protect systems from unauthorized access. Antimalware software (antispyware/antivirus applications) protects systems from malware.

## Firewalls

A *firewall* is a security barrier that prevents unauthorized access to or from private networks. A firewall can prevent outside users from accessing proprietary data on the corporate network from the Internet. Firewalls are also used to control employee access to Internet resources.

A firewall works by monitoring and regulating traffic between two points, such as a single computer and a network server. Firewalls can be implemented through hardware or software.

When you connect your computer to the Internet, you are potentially connecting to all the computers on the Internet. This relationship works in reverse as well: All other computers on the Internet are connected to yours, and perhaps to all the computers on your corporate LAN.

By connecting to the Internet through corporate firewalls, no computer on the LAN is actually connected to the Internet, and any requests for information must pass through the firewall. This feature allows users on the LAN to request information from the Internet, but to deny any requests from outside users for information stored on the LAN.

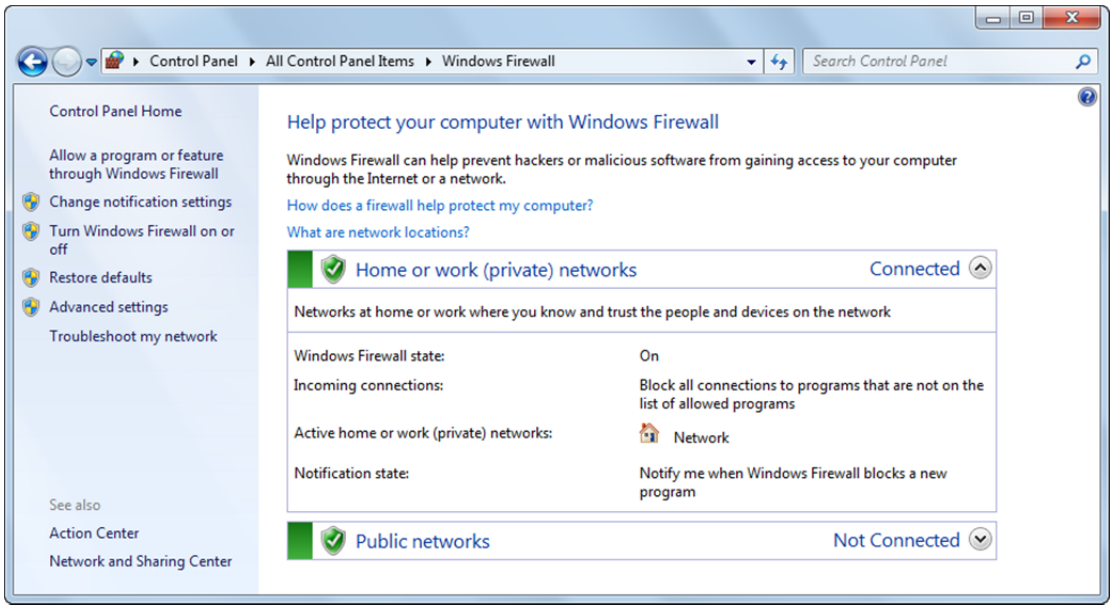
Firewalls can be considered the first line of defense against LAN security breaches because they provide data confidentiality. Firewalls do not ensure data integrity because they do not encrypt or authenticate data. In many corporate settings, one firewall protects all the stations on the LAN.

### Desktop Firewalls

Also known as personal firewalls, desktop firewalls offer protection for an individual system instead of an entire network. Tools such as Norton 360 or ZoneAlarm Internet Security Suite can detect and respond to attacks on a computer system.

Desktop firewalls offer many firewall features, such as inspection of all incoming transmissions for security threats. When a firewall is used in conjunction with antivirus software, a personal computer is secure, provided that the user updates these applications frequently.

Many operating systems now include built-in (native) desktop firewall software. Windows, for example, includes Windows Firewall which is enabled by default. You can configure the Windows Firewall to suit your needs, and you can turn it on or off. The Windows Firewall is shown in the following figure.



## Antispyware

You can detect the presence of spyware by purchasing a spyware detection application, or by using Windows Defender. Antispyware applications scan a computer's hard drive, memory and network connections, and look for suspicious activity.

Spyware detection applications contain lists of known spyware. These lists are known as definitions. As new forms of spyware emerge, the application vendor updates the definitions and makes them available for download and installation. Most antispyware applications can be configured to look for and install updated definitions automatically. It is very important to keep antispyware software updated.

Network and systems administrators can detect the presence of spyware by doing the following:

- Using a network analyzer to capture and study network transmissions for suspicious packets.
- Using the netstat utility to review all open ports. (Netstat is a TCP/IP utility that reads network data structures.) If the administrator finds a suspicious port open on the system, he or she can conduct a web-based search on that port. The administrator may discover that it is a port used by spyware installed on the system.

End users can combat spyware by:

- Deleting the application that contains the spyware.
- Using a desktop firewall to block transmissions between the system and the spyware vendor.

## Antivirus Software

The best protection against a virus is to know the origin of each program or file you install on your computer, or open from your email or instant message client. However, because knowing the origins of everything is nearly impossible, use antivirus software to scan email attachments and files for known viruses, and to eliminate any viruses that are discovered.

*Antivirus* applications are available from many vendors. Some include freeware versions of their programs as well as enhanced versions for purchase. All versions include free and frequent updates to the virus definition files that enable the program to recognize and remove the latest viruses.

Some popular antivirus programs include:

- AVG
- Avast
- Avira
- ClamWin
- McAfee
- Microsoft Security Essentials
- Norton Antivirus/Norton 360

As soon as you install antivirus software, scan the computer for any possible viruses that could already be resident, and subscribe immediately for automatic updates (or notices of updates) for the virus definition files and patches for the program. It is generally a good practice to scan the system again after updates are installed. It is important to schedule regular system scans and to configure the application to automatically scan email messages as they are delivered to your Inbox.

If and when a virus is detected, you can use the antivirus software to disinfect the system. Antivirus software that is kept current knows the signatures of the latest viruses, and works by scanning the infected file or program for these known signatures. If the virus is found, your hard drive can often be disinfected immediately so that the virus cannot infect other files or cause more damage.

When an antivirus program is running, it will scan the files you select; when it finds a virus or threat, it will give you the option to quarantine or remove the threat.

- If you elect to quarantine the infected files, the antivirus program will place the infected file in a quarantined or vault area where it cannot infect other files. Quarantined files can usually be deleted at any time.
- If you elect to remove the file, the antivirus program will permanently delete this file from your system. You usually do not need to do anything else.
- If the antivirus finds a virus that cannot be removed, it will still quarantine the infected file. You may be able to find a removal tool for this virus on the antivirus program's website. Generally you will need to download a file and then follow the instructions for removing the virus from your system. Alternatively, you may need to research how to remove the infected file manually.

- If the virus is in active memory and you are not able to launch the antivirus software, turn off the computer and reboot from a known, clean bootable disk to start the system without the virus in memory. You should then be able to launch the antivirus software and begin the disinfection process.
- Remember to check all your disks and backup files with the antivirus software, and remove the virus from them if necessary.
- Replace any file or programs that have been damaged or changed by the virus with backup copies or reinstall programs from original installation media.
- Be sure to find and remove all copies of the virus on your system.

It bears repeating that it is extremely important to keep antivirus software up to date and configured to automatically download updates. It is equally important to keep the email scanner and resident scanner portions of the application turned on. Regular system scans are recommended, and these can be scheduled. You can also manually start a scan at any time.

### Avoiding Viruses

Conducting regular scheduled scans, and enabling the resident scanner and email scanner portions of the application can provide reasonable assurance that a system is not infected. Other steps to take to avoid infection include:

- Saving files you download from the Internet to a folder other than your data folder. Scan all downloaded files before opening them, especially if they are executable files.
- Scan any removable media (CD, DVD or flash drive) before copying or opening files contained on the media.
- If you share files with other people using portable devices, scan any files you plan to give to others to ensure you do not inadvertently pass a virus on to them.
- Because email is the most common method for spreading viruses, always set your antivirus program to automatically scan all incoming and outgoing messages.
- Always scan email attachments before opening them, even if they come from someone you know.
- Be suspicious of any unexpected attachments you receive with email or instant message transmissions. If you receive an attachment you did not expect or do not recognize:
  - Do not open the attachment.
  - Try to contact the message sender (using a method other than email) and determine whether the attachment is legitimate.
  - If you are unable to contact the sender or the sender is unaware of the attachment, delete the attachment from the message.
  - Open your Deleted Items folder and delete the attachment from it to permanently remove the attachment from your system.

The best protection is prevention. But if your system is infected, most viruses can be removed without permanent damage.

## Maintaining a Secure Environment

Prevention is always preferable to repair. Two simple ways to keep these systems secure is to schedule regular scans and to ensure that application and operating system updates are installed as required. Updates will be covered in detail later in this lesson.

Regularly scheduled scans can easily be configured on corporate systems. To avoid interfering with an employee's ability to work, scans can be scheduled to occur after normal working hours (for example, you can schedule a scan to begin at midnight).

As a member of the IT staff, you should periodically view the quarantine files on corporate systems to see how much virus activity has been discovered and possibly to identify systems that are more at risk than others. If it is discovered that employees are turning off scheduled scans, the rights on the system can be adjusted as appropriate. Limiting a user's rights on a computer can be a sensitive area, however, and increasing user awareness and education may provide better results

To keep track of portables, you may need to require employees to periodically bring in their laptops for routine maintenance.

## User Awareness and Education

No matter how tight a security policy may be, it is only effective if people adhere to it. The first step in securing any network is to educate the people who use it.

If you restrict services such as instant messaging on your network or require that all browsers suppress pop-ups, it is important to make sure the employees understand why. If they do not understand the risks that prompt these tight security measures, they are likely to try to find ways around them.

Educate users about the signs of virus infection or spyware infection, and instruct them to notify someone in the IT department immediately. An alert user can provide an early warning that a network-wide infection may be in progress, and IT can respond proactively instead of reactively, possibly tracking down and isolating the source of the infection and documenting the probable source and the applied treatment. Having a record of past infections and treatments can be a valuable tool for a network administrator facing a new infection or attack.

While the reasoning behind the rigors of a strict security policy may make sense to IT personnel, the average user may not understand and may even resent them, and consequently look for ways around them. An informed workforce will make the best ally. In general, make sure that users understand:

- How to protect their user names and passwords. If necessary, explain that passwords should not be written down on a slip of paper and "hidden" beneath the computer keyboard.
- How to create a complex password of sufficient strength.
- Why they may be required to periodically change their passwords.
- Why they should always keep the antivirus software running and resident.
- How to recognize signs of a virus infection or signs of spyware infection.
- How to manually start antivirus scans.
- Why they should not indiscriminately click links in pop-up windows or instant messaging applications.
- How to avoid poisoned websites.
- Why certain applications may be prohibited on corporate systems.

# Microsoft Malware Solutions

Objective 3.3 6.2

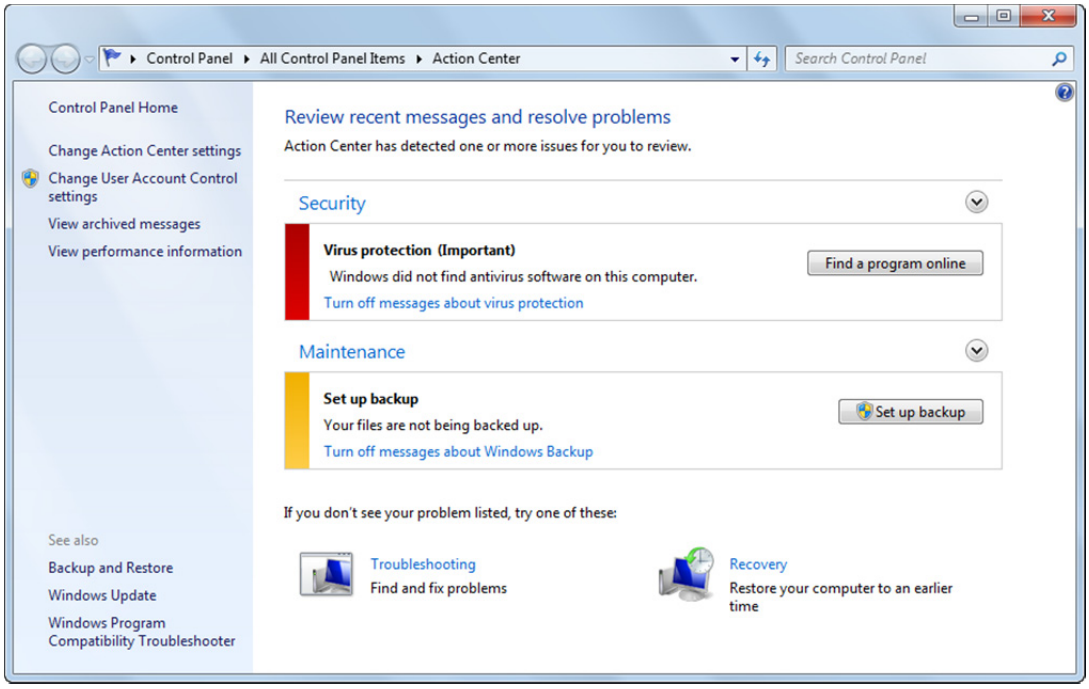
Microsoft provides various tools to help protect systems from malware and to remove malware should a system become infected. Some of these tools are included with Windows 7, while others must be downloaded or purchased before use.

## The Action Center

While the Action Center doesn't actually protect a system from malware, it does provide notifications related to antimalware software installation and update status. For example, the Action Center will notify you if you have no antimalware software installed or if the definitions are outdated.

You can access the Action Center by clicking on a notification balloon, or through the Control Panel. It provides a central place to view alerts and take actions that can help keep the system secure. The Action Center lists important messages about the current security and maintenance settings that require attention.

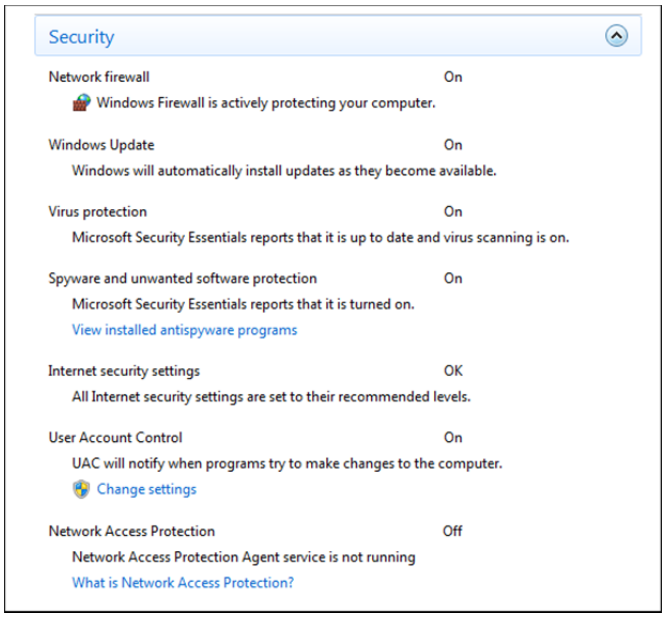
The following figure shows the Action Center.



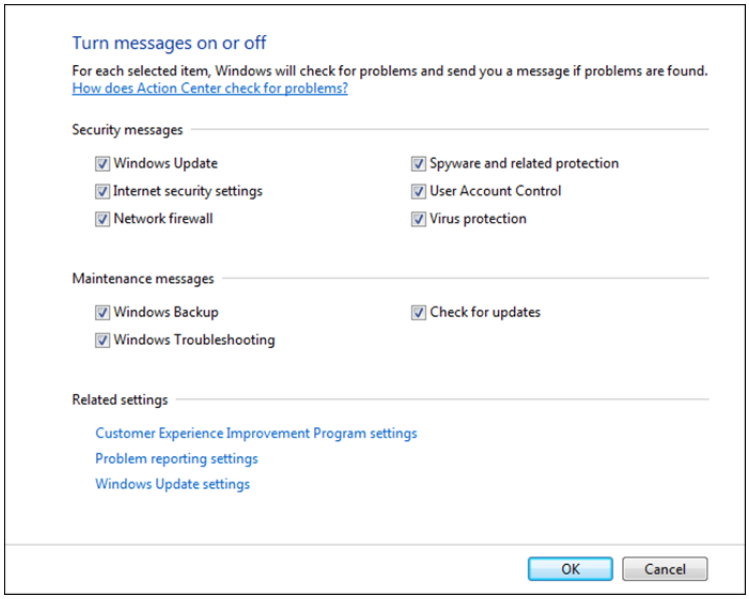

Red items in the Action Center are labeled important and indicate significant issues that require fairly immediate attention. Yellow items are suggested tasks that you should consider addressing.

If you expand the Security section, the Action Center will notify you about the status of the following security features:

- Windows Update
- Internet security settings
- Network firewall
- Spyware protection (Windows Defender)
- User Account Control
- Virus protection



You can change the notification settings by clicking the **Change Action Center settings** link. Use this page to turn messages on or off.




## Malicious Software Removal Tool

The Malicious Software Removal Tool (MSRT) is a free download from Microsoft that removes over 160 known malware applications. The MSRT checks computers running Windows 7, Windows Vista, Windows XP, Windows 2000, Windows Server 2003 and Windows Server 2008 R2.

Microsoft releases an updated version of this tool on the second Tuesday of each month and as needed to respond to security incidents. The tool is available from Microsoft Update, Windows Update and the Microsoft Download Center.

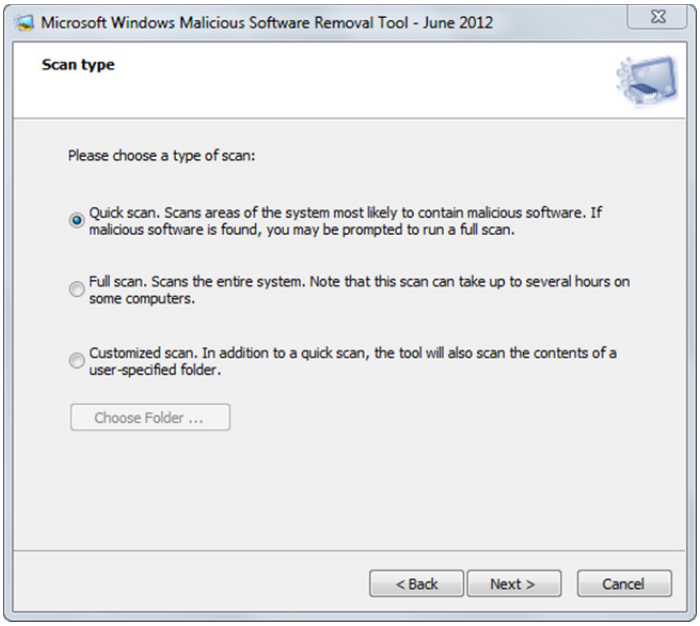
The Microsoft Update/Windows Update version runs in the background once each month and reports if a malware infection is found. The version available at the download center can be executed whenever necessary.

## Exercise 6-1: Downloading and Using the MSRT


In this exercise, you will download the MSRT and check for malware. You can run it using either a standard user or administrative user account.

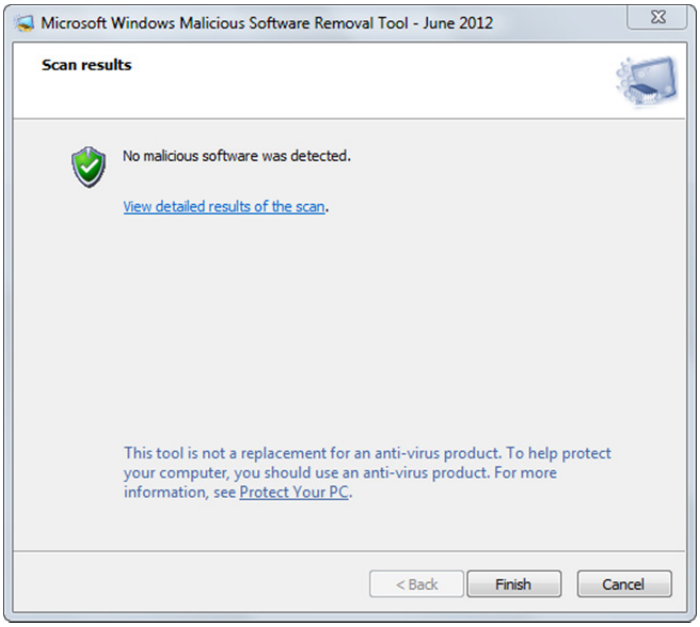
1. Open a web browser and navigate to www.microsoft.com/security/pc-security/malware-removal.aspx.
2. Click the **Skip the details and download the tool** button.
3. Ensure that the correct language is selected.
4. If you have a 64-bit operating system, scroll down to the Overview section, then in the second paragraph, locate the text that reads: To download the x64 version of Malicious Software Removal Tool, click **here** and click the link.
5. Click the **Download** button.
6. A page suggesting additional products may appear. If it does, click **No thanks and continue** to skip the suggested additional products, then click **Save** when prompted to Run, Save or Cancel the download.
7. When the download is complete, click **Run** and click **Yes** when prompted by the User Account Control.

8. Read the welcome screen, then click **Next**.




9. Ensure that Quick scan is selected, then click **Next**.

   The scan may take a few minutes. When the scan is complete, the MSRT displays a report of its findings.




10. Click **Finish**.
11. Close your browser.

In this exercise, you downloaded the MSRT and scanned for malware.

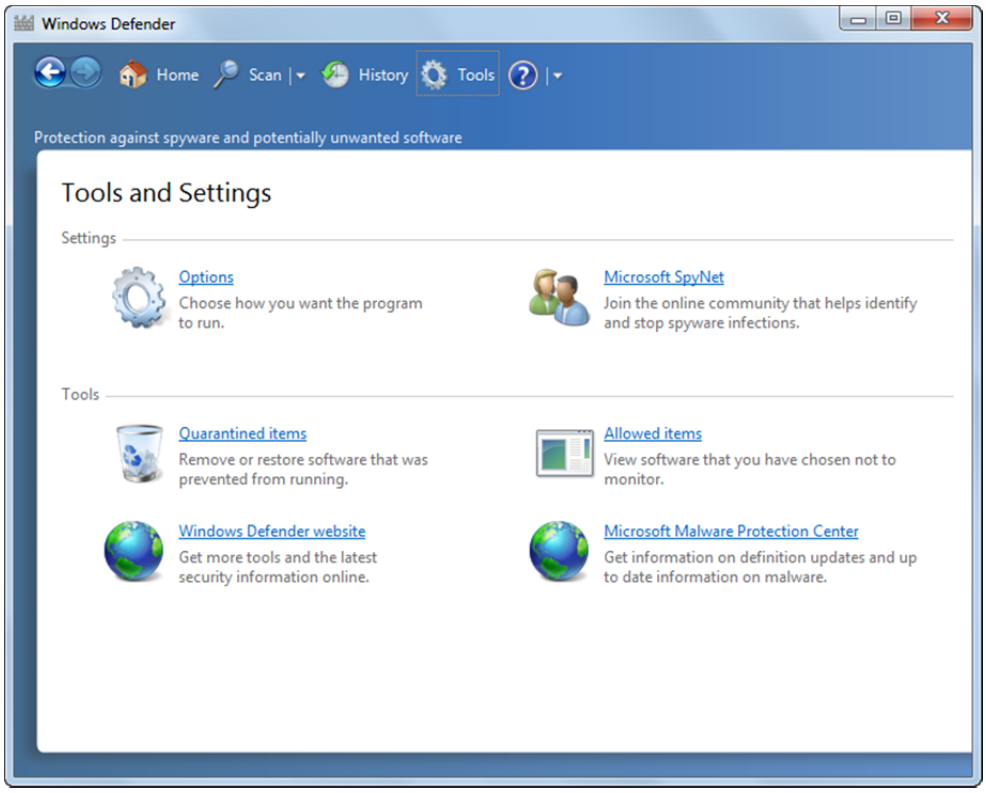
# Windows Defender

Windows Defender is a pre-installed antispyware application that comes with Windows 7. It detects and removes known spyware from a client system. Defender runs automatically when it's turned on and offers:

| | |
|---|---|
| **Real-time protection** | Defender alerts you when spyware attempts to install itself or to run on your computer. It also alerts you when programs attempt to change important settings. |
| **Scanning options** | You can scan for spyware that might be installed on your computer, schedule scans on a regular basis, and automatically remove anything that's detected during a scan. |

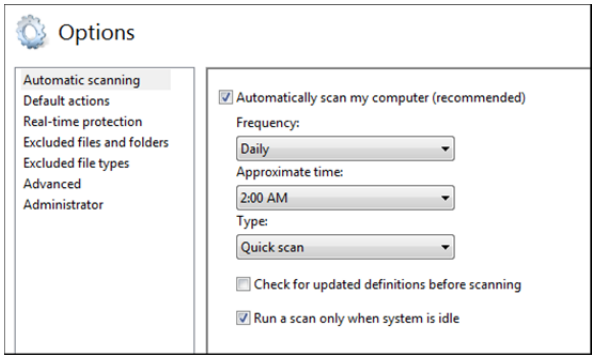
Spyware-detection applications can report false positives, in which legitimate applications are incorrectly categorized as spyware. As you use a spyware-detection application, be sure to examine the results carefully so you do not remove legitimate applications.

You can use the Tools and Settings screen to configure specific options, view and work with quarantined items, and indicate specific programs that you want Windows Defender to ignore.

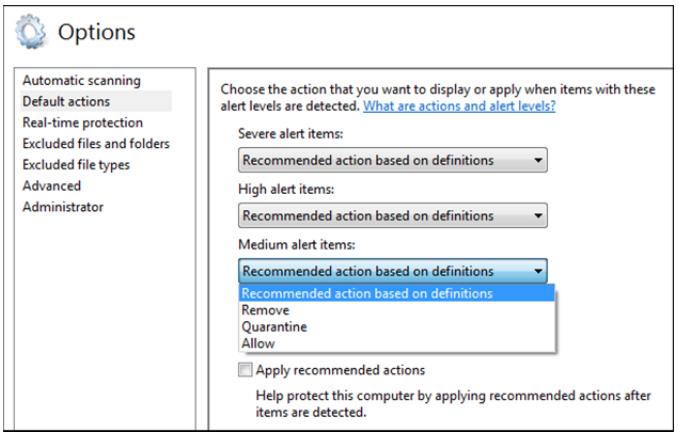



You use the settings on the Options screen to configure:

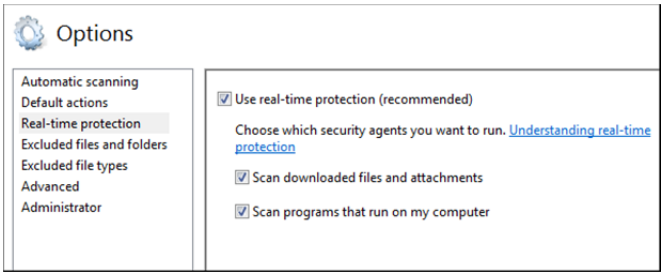
**Automatic scanning** – set the frequency, time and type of scan to perform. You can also specify to check for updated definitions before running an automatic scan.



**Default actions** – specify what Windows Defender should do when it encounters items at specific alert levels. The available options for Severe alert and High alert items are Remove and Quarantine. The options for Medium alert and Low alert level items are Remove, Quarantine and Allow.



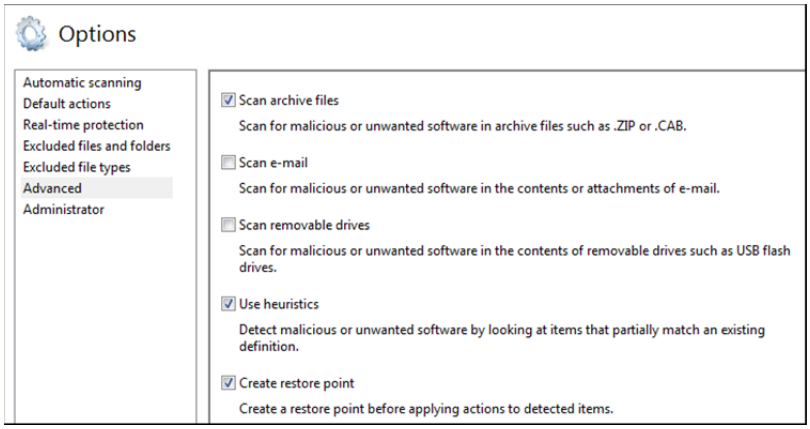

**Real-time protection** – specify whether you want to use real-time protection and specify which security agents you want to run. Real-time protection runs in the background and monitors downloaded files and attachments and/or programs that are running on the system.




**Excluded files and folders** – specify files or locations not to scan.

**Excluded file types** – specify types of files not to scan.

**Advanced** – specify which files to scan. You can also specify to create a restore point. Restore points allow you to return a system to a previous configuration. You will learn more about restore points later in this lesson.




**Administrator** – specify to turn Windows Defender on or off and whether to view items from all users or only the current user.

Defender can be configured to work with Windows Update to automatically install new definitions as they're released. You can also manually check online for updated definitions before scanning.

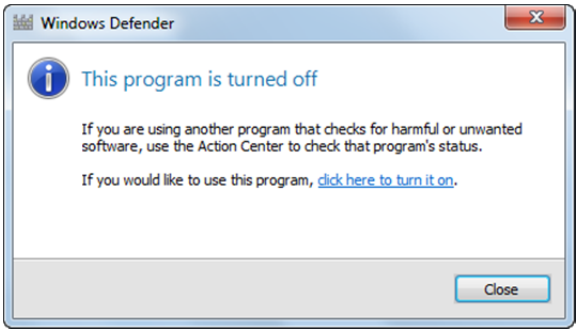
If you plan to install another antivirus/antispyware application on the system, it is recommended that you turn off Windows Defender to avoid conflicts. Some antivirus applications automatically disable Windows Defender when they are installed. Some antivirus applications such as Microsoft Security Essentials must be uninstalled before Windows Defender can be re-enabled.

# Exercise 6-2: Using Windows Defender (Optional)

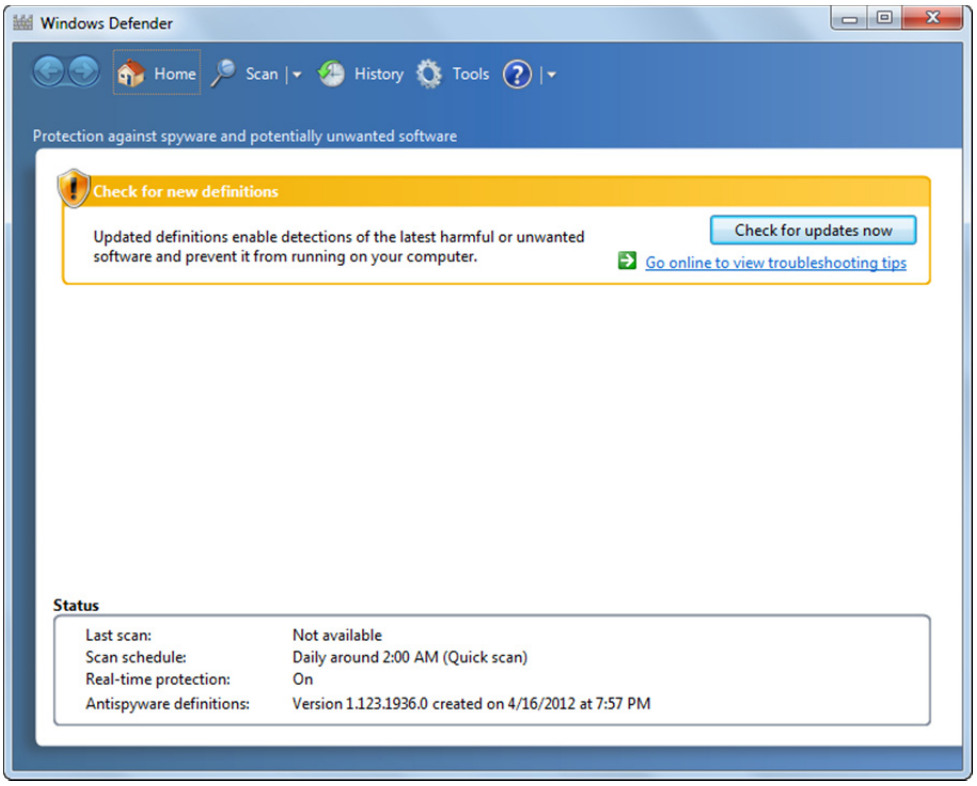
In this exercise, you will turn on Windows Defender (if necessary), look for updates and scan the system.

Note that certain antispyware/antivirus programs will not allow you to turn on Windows Defender. For example, if Microsoft Security Essentials is installed, you will be unable to turn on Windows Defender. Ask your instructor before performing this exercise.

1. Open the Control Panel, change to Large or Small icons view if necessary, then click **Windows Defender**.
2. If Windows Defender is turned off, the message box shown will appear.




3. Click the **click here to turn it on** link to open Windows Defender.



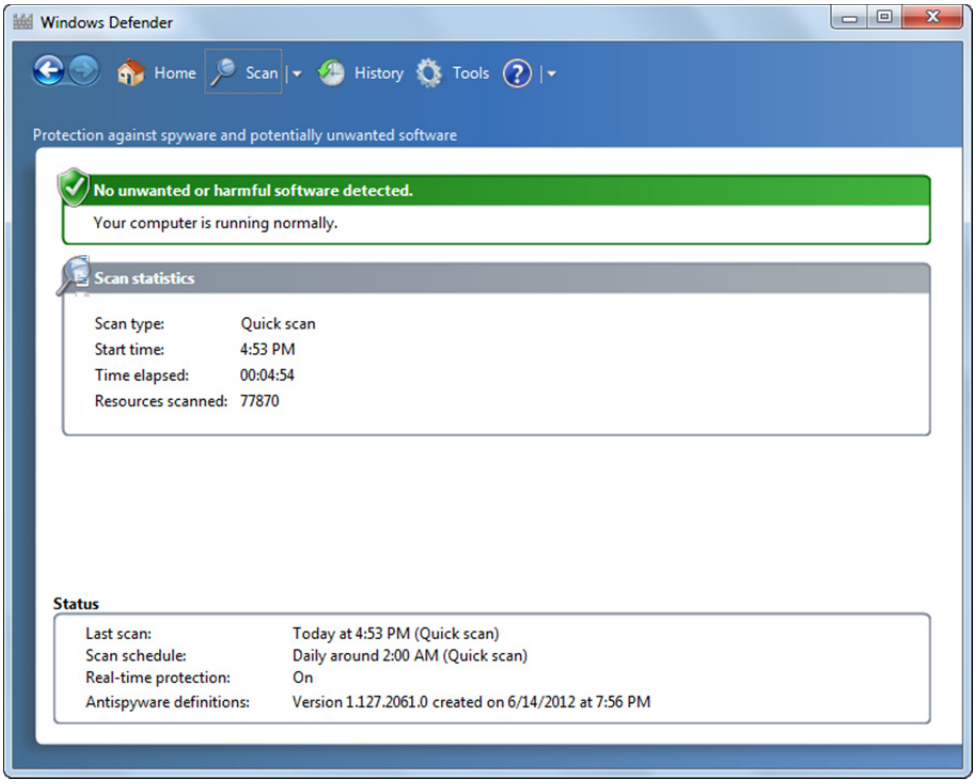

If Windows Defender had not previously been turned on, or has not been used for a while and is not configured to automatically search for updates, you can click the **Check for updates now** button.

4. If the Check for updates now button is not visible, you can still manually check for updates. In the toolbar at the top of the window, click the drop-down arrow to the right of the **Help** button and select **Check for updates**.

   It may take several minutes for updates to be downloaded and installed. When Windows Defender is up to date, the Status will indicate either that the program is up-to-date or that no new definitions or updates are available.

5. To begin a scan, click the **Scan** button in the toolbar.

The scan may take a few minutes. When complete, Windows Defender will display the scan results.




6. In the toolbar, click the **Tools** button to open the Tools and Settings window.
7. Take some time to explore the options presented in the Tools and Settings window, then click the **Options** link to open the Options window. Take some time to explore these settings.
8. In the left pane of the Options widow, click the **Administrator** link, then clear the **Use this program** check box.

   Clearing the check box turns Windows Defender off. In many cases, antivirus programs also scan for spyware, and it is not recommended that you run two antispyware applications at the same time.
9. Click the **Save** button
10. When the notification that Windows Defender has been turned off appears, click the **Close** button.
11. Close the Control Panel.

In this exercise, you turned on Windows Defender, downloaded and installed updated definition files, scanned the system and turned Windows Defender off.

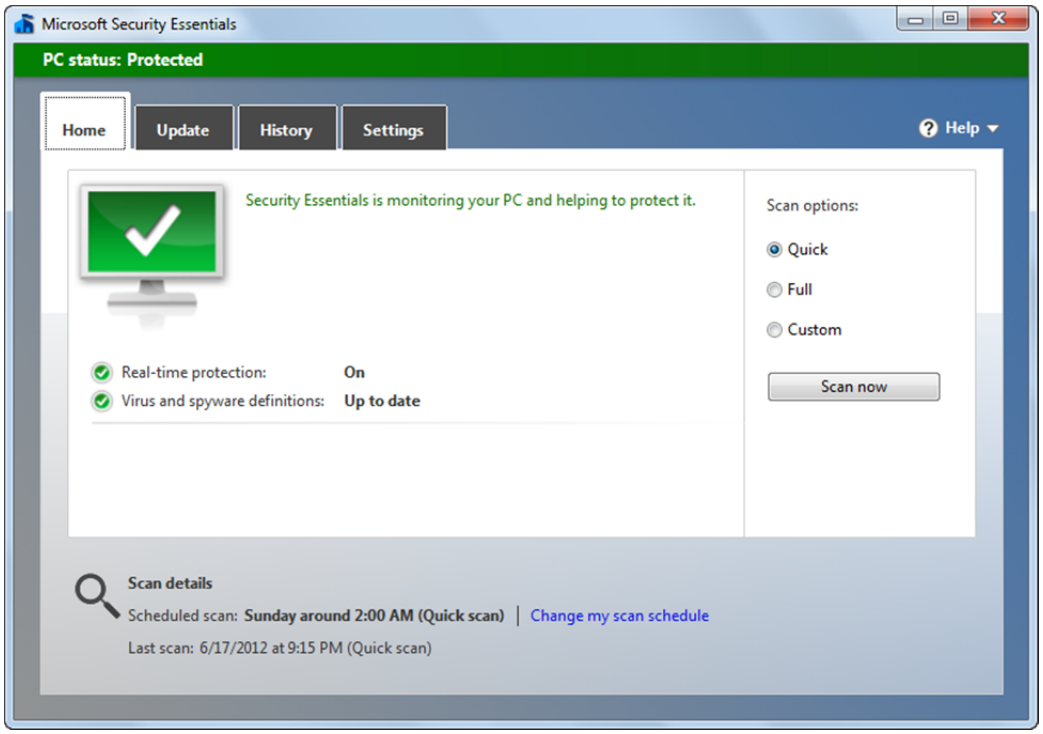
Check with your instructor before turning off Windows Defender.

## Microsoft Security Essentials

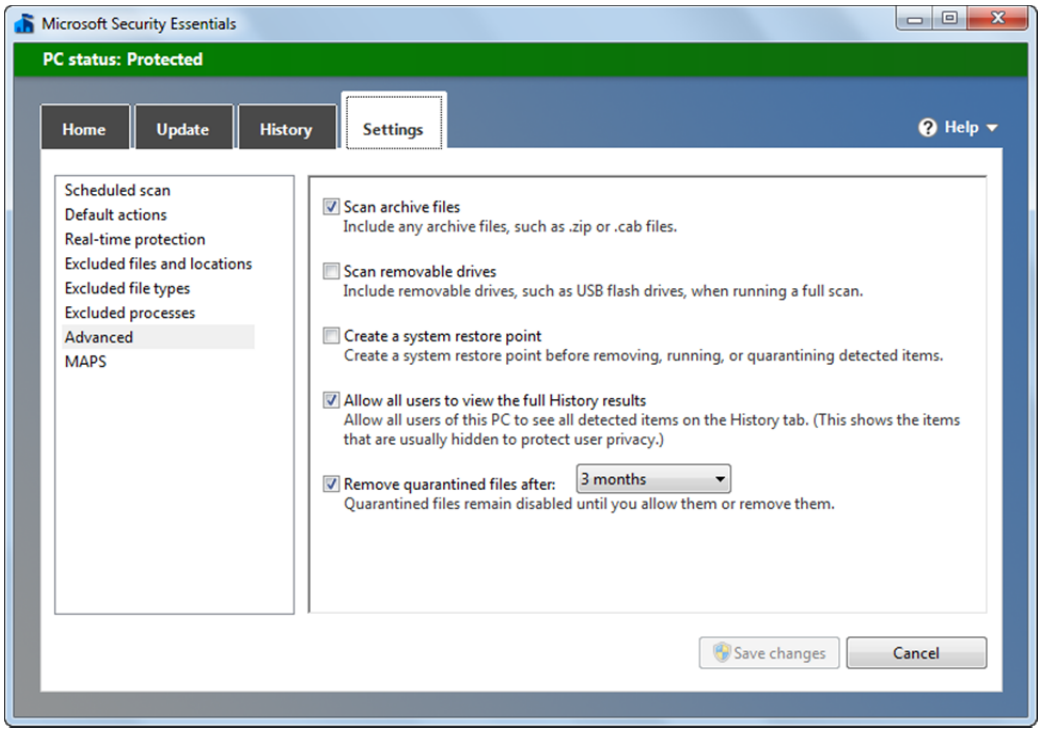
Microsoft Security Essentials is a free antimalware application that you can download from: www.microsoft.com/en-us/security_essentials/default.aspx.

Once installed, it actively monitors the system processes and files, scanning for malware. The following figure shows the Microsoft Security Essentials home tab.

**MMM**
Using Microsoft Security Essentials




Like Windows Defender, Microsoft Security Essentials can be used for real-time protection and scanning-based protection. The Settings tab provides virtually the same options as Windows Defender.




Microsoft Security Essentials is free for home use and for business use for up to ten PCs.

# Microsoft Forefront Endpoint Protection

Microsoft Forefront Endpoint Protection is an award-winning product that protects against computer viruses and other forms of malware and is designed specifically for use within an enterprise.

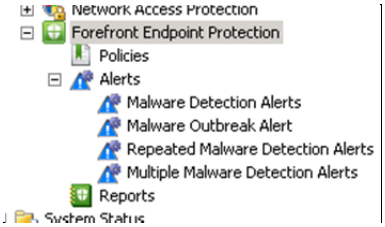
In an enterprise, security protection must be deployed in multiple layers. For example, to protect against viruses being pushed to your computer from the Internet, you should use a router with a built-in hardware firewall. Another key component in multi-layered protection is the use of antivirus software on every *endpoint*. An endpoint is any intelligent computing device (such as a server, desktop or laptop computer, tablet, or handheld computer that has a CPU and is capable of running application software) connected to others in a network. A successful virus attack on any endpoint can easily result in an outbreak to the other endpoints; your defense is only as strong as the weakest link in the entire network. Businesses with more than 10 computers can purchase Forefront Endpoint Protection (FEP) from Microsoft to manage all of their endpoint devices.

FEP is designed for medium-size and large enterprises. Imagine that you are the system administrator for an enterprise. It is your job to ensure that antivirus software is installed, configured and maintained on every endpoint in the enterprise. You already know that many users fail to download and install virus definition updates and that some even turn off their antivirus protection. Even in a relatively small enterprise of 50 systems, ensuring protection on all the endpoints is a time-consuming, and likely frustrating, task. How much more difficult would this job be if your enterprise consisted of thousands of computers spread around the nation?

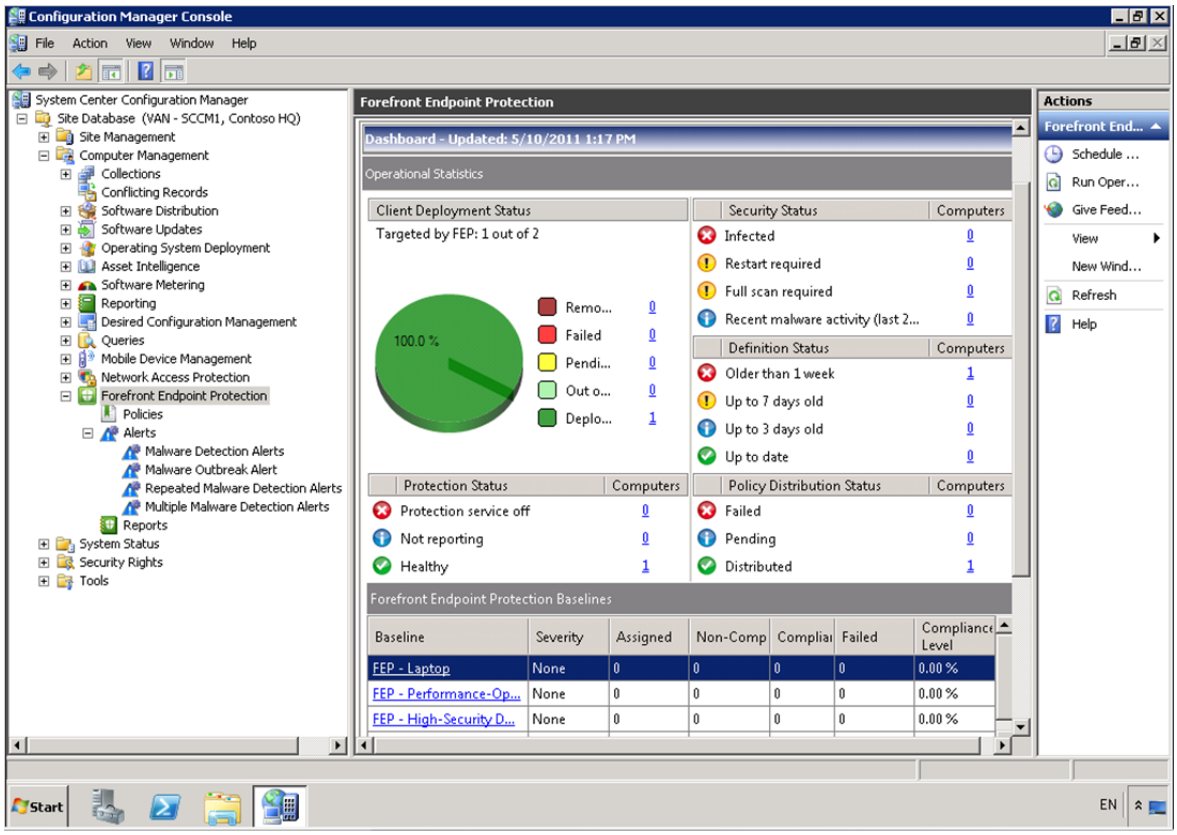
Microsoft's FEP is an award-winning product that protects against computer viruses and other forms of malware. Instead of building a separate system solely for managing this product on its own, it is built into the Microsoft System Center Configuration Manager (SCCM, also known as ConfigMgr or formerly as System Management Server) so that system administrators and security administrators can both – or independently – ensure the software is working properly on all endpoints and that updates are regularly applied.

This is an important advantage because a massive virus outbreak must be contained quickly, and system administrators are usually the first to respond and cannot wait for the security administrators to arrive. Another important advantage of being built into SCCM is that the highly efficient design enables all endpoints to be managed from a single central console. This design enables a network of any number of endpoints (e.g. tens of thousands) to be monitored and updated with very little effort.

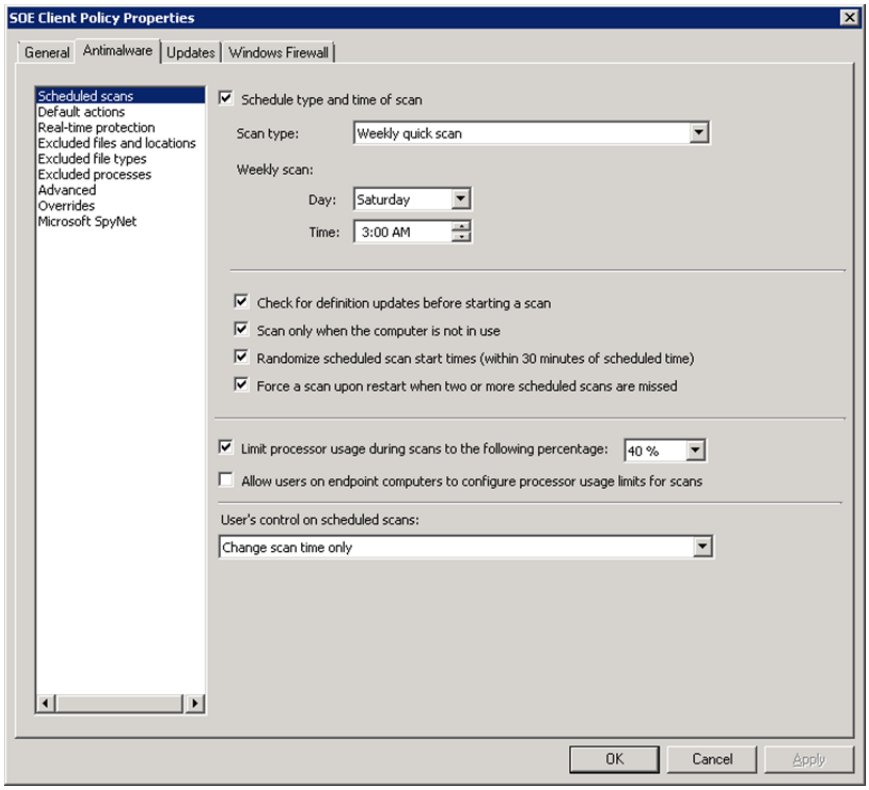
The following screenshot shows the options available under FEP:



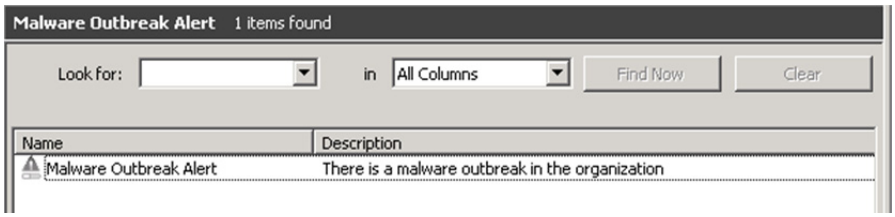

When you select a main item in the tree, a dashboard is displayed, which provides administrators a global view (e.g. using the green/yellow/red color scheme) and selected statistics for the enterprise. Administrators can determine the overall health of the network with just a quick glance using this window.



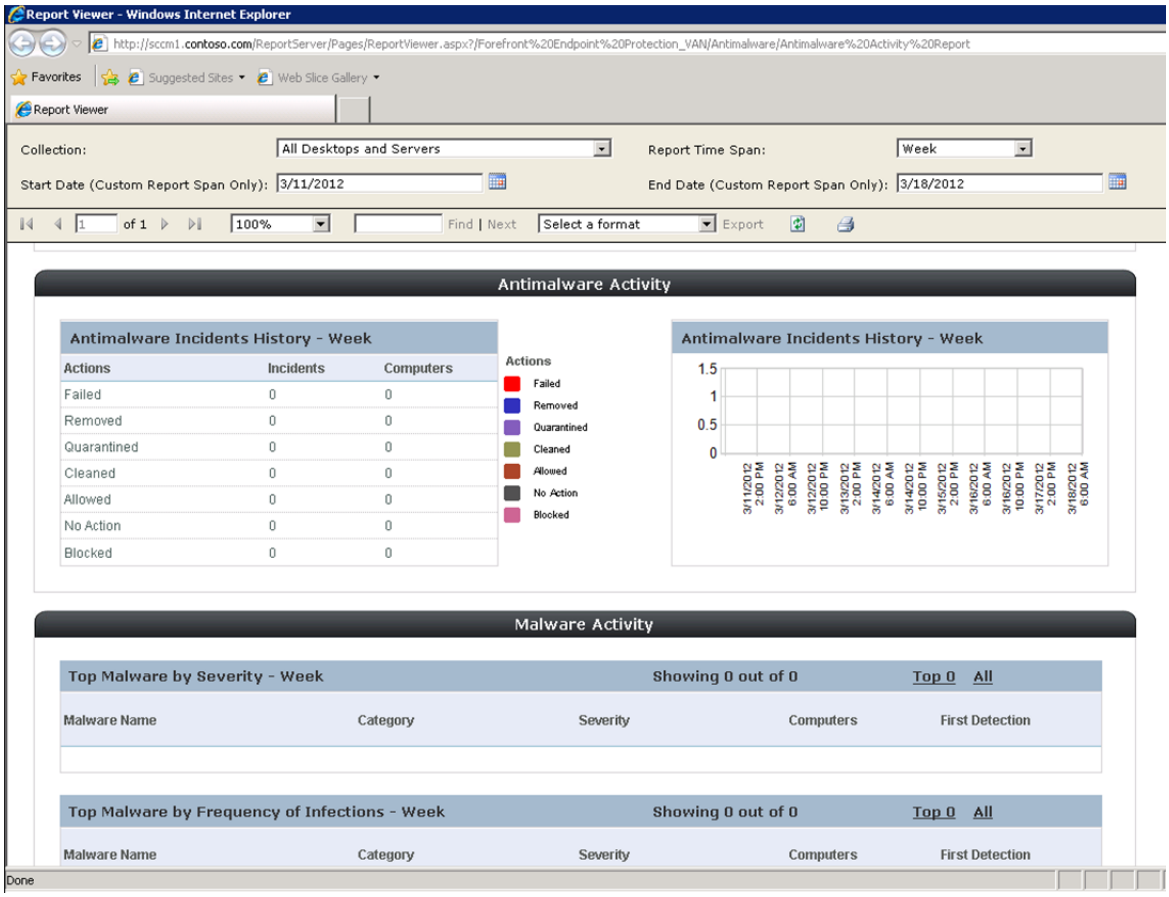

Different policies can be set up within FEP to handle the different antimalware protection settings for different groups of endpoints. For example, all servers in the head office may require a weekly scan on Saturday starting at 3:00 AM:



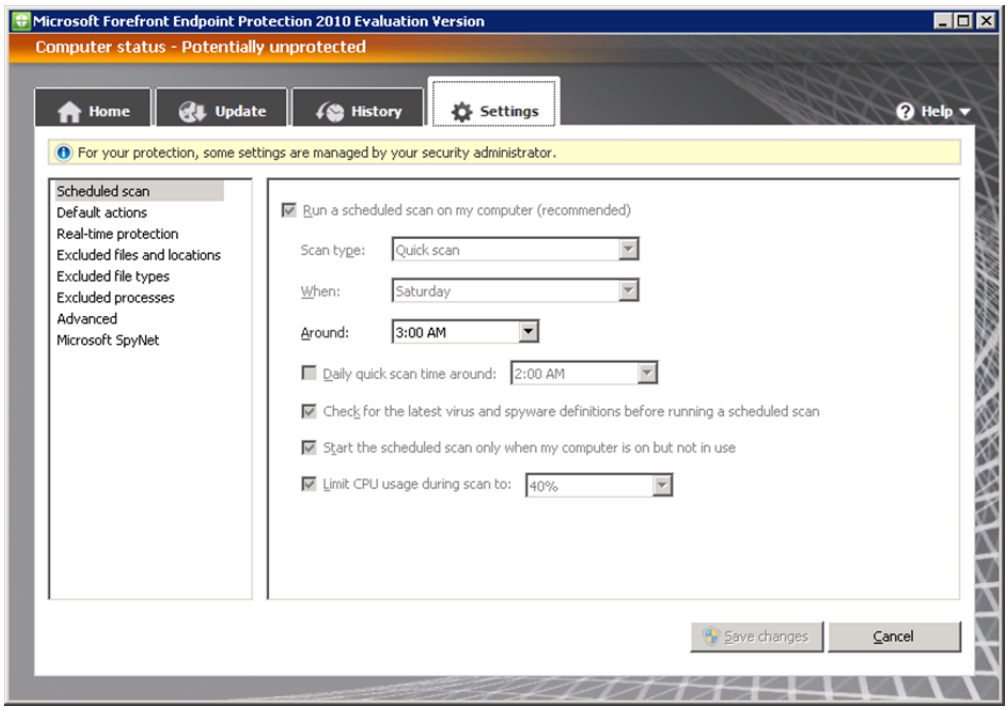
FEP can be configured to generate alerts immediately whenever an outbreak occurs. The alerts are sent via email to a selected group of administrators:




Reports can also be set up to monitor activity during any given time period:




On endpoint systems, the FEP software locks many of the option settings because these are managed by the system administrator.




The overall design creates a good balance between end users and security administrators. Users are able to concentrate on their own tasks without having to worry about maintaining the security of their systems. Security administrators can be confident system security is maintained consistently on every endpoint.

One of the Microsoft websites offers a hands-on demonstration (called virtual labs) of setting up, managing, and using ForeFront Endpoint Protection. Navigate to http://technet.microsoft.com/en-us/virtuallabs/ and select the Forefront Security link.

# Windows Backup Methods and Tools

Objective 6.1

A system is useful only if the data it contains is valid and accessible. You can take several steps to ensure the safety of data. Perhaps the most obvious way to protect data is to schedule regular backups and to closely follow corporate guidelines regarding backup procedures. A *backup* is a duplicate copy of a program, a disk, or data, made either for archiving purposes or for safeguarding files from loss if the active copy is damaged or destroyed.

The backup methods available for Windows 7 systems fall into the following basic categories:

| | |
|---|---|
| **Local** | These are backups stored on removable media on local external drives. |
| **Online** | These are backups stored to a remote location on the local network, or those created with Internet-based backup services through an encrypted session. |
| **Cloud backup** | A variation of an online backup wherein data is saved to a cloud location such as Microsoft SkyDrive. |
| **Automated** | These are recovery options that create automatic backups for disaster recovery. |

Windows 7 includes several tools for creating backups. These include: file backups, system image backups, previous versions and system restore points.

# Backup and Restore Utilities

Keeping a current backup of all data files is essential to ensuring that data can be recovered in the event of a failure. You use the Backup and Restore utilities to back up and recover files and folders. When you back up data, you store copies of folders and files to a source other than your computer's hard disk. Depending on file size and available hardware, target storage locations can include:

- Internal hard drives (other than the drive on which Windows is installed)
- External hard drives
- Network locations – supported only in Windows 7 Professional, Enterprise and Ultimate. The user must have full control on the destination share.
- USB flash drives
- Writeable CDs, DVDs, and Blu-ray Discs

Note that target volumes must be formatted as NTFS, FAT or UDF. The drive being backed up cannot be the target, and the Windows volume cannot be the target. Similarly, a recovery partition cannot be the target, nor can a locked BitLocker partition.

The Backup and Restore utility can be used to back up the entire system or only the files and folders you select. You can allow Windows to choose what to back up or you can select the individual folders, libraries and drives that you want to back up. By default, backups are created on a regular schedule. You can change the schedule, and you can create a backup manually at any time. Once you set up Windows Backup, Windows keeps track of the files and folders that are new or modified and adds them to your backup.

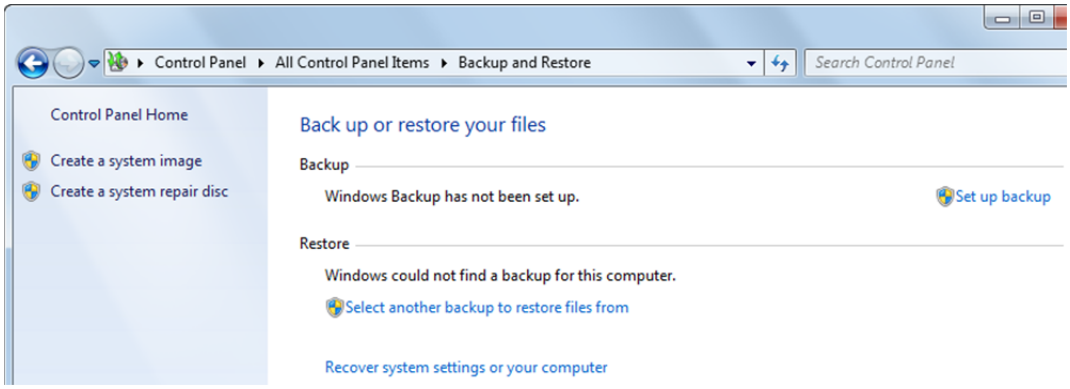
If you have never used Windows Backup before, you need to set it up first, and then follow the steps in the wizard.

## Exercise 6-3: Backing up Data


In this exercise, you will back up data using the Window Backup utility.

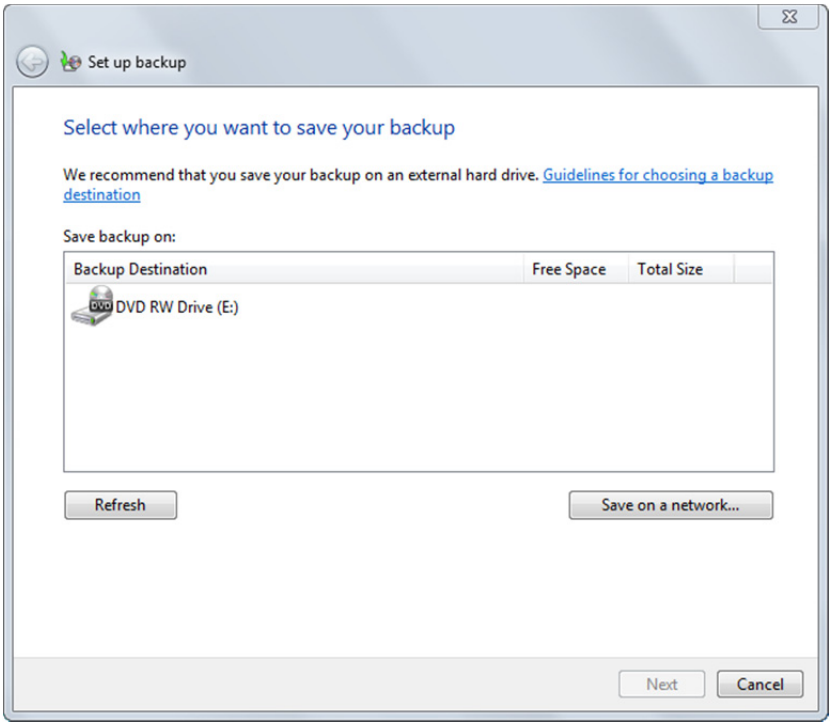
This exercise requires a CD or DVD burner and a blank recordable disk, or a flash drive for each student station.

1. Open the Control Panel, change to Large or Small icons view if necessary, then click **Backup and Restore** to open the Backup and Restore window.

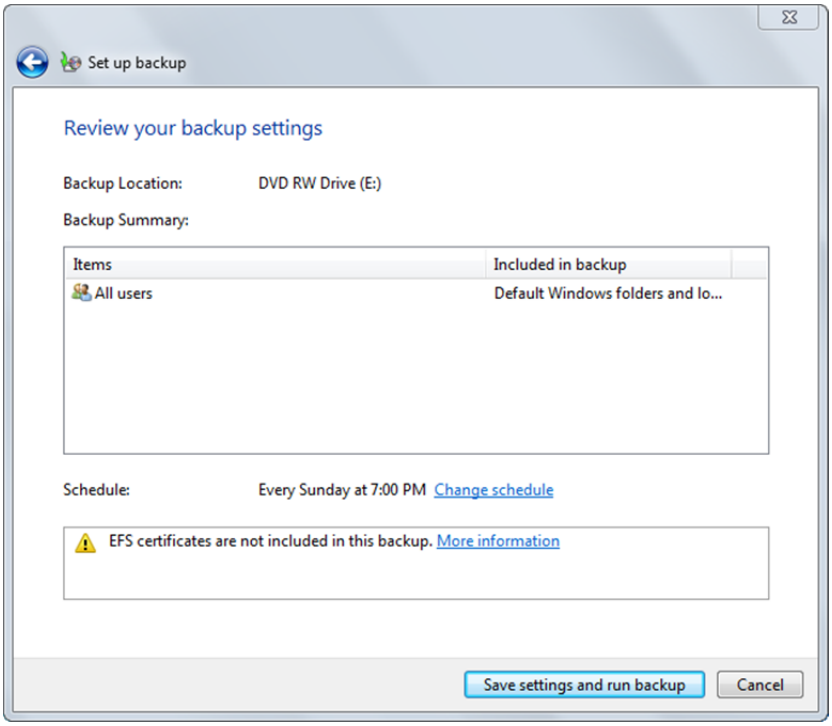



If Windows Backup has not been set up, you can set it up by clicking the **Set up backup** link.

2. Click the **Set up backup** link to open the Set up backup window.

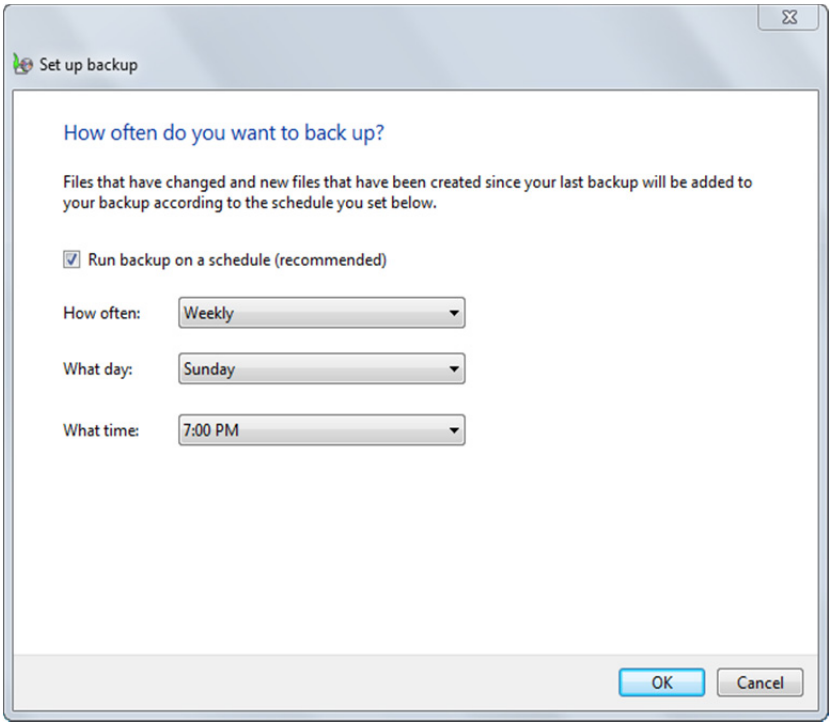



3. Click a location in the **Backup Destination** list box, then click **Next**.
4. When asked what you want to back up, accept the default setting for letting Windows choose. This option backs up files saved in libraries, on the Desktop and in default Windows folders. Click **Next**.

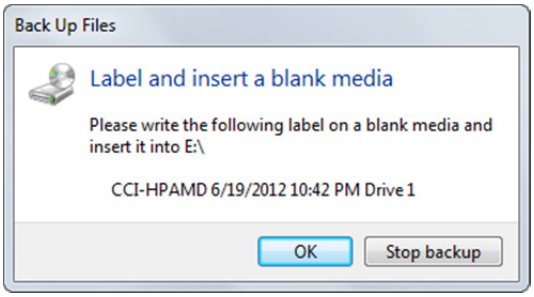



You can save the settings and run the backup immediately, or you can click the **Change schedule** link to edit the configuration.

5. Click the **Change schedule** link.




6. Use the drop-down lists to configure the backup the way you want it, then click **OK**.
7. Click the **Save settings and run backup** button. Windows Backup begins to run in the background. If you selected an optical drive as a backup location Windows will prompt you to label and insert a blank disc.

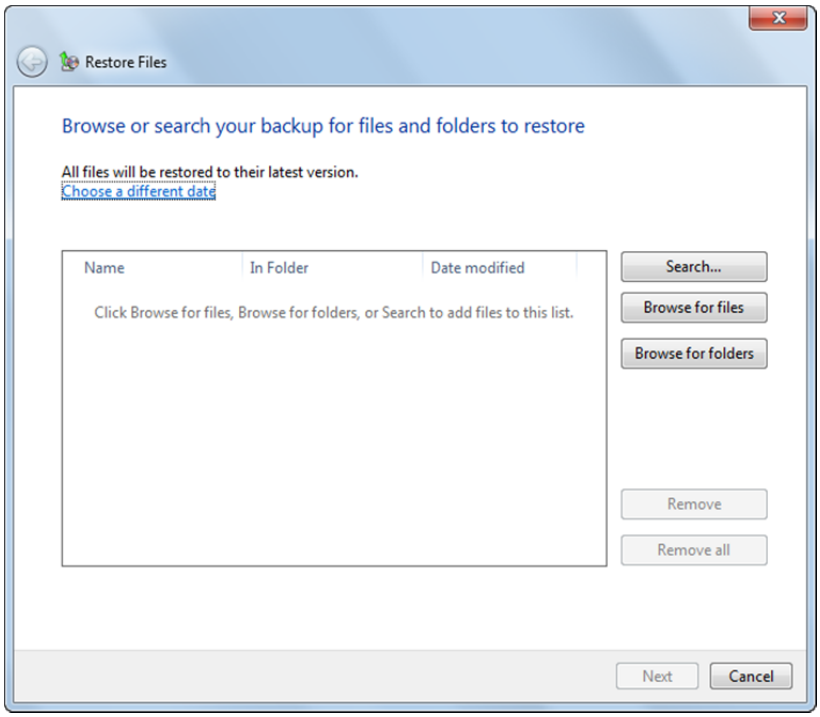



8. If you have blank disc, insert it into the optical drive and click **OK**. (If you do not have a blank disc, click the **Stop backup** button.)
9. If prompted to format the media, click the **Format** button (Windows may format the media automatically). If prompted, insert additional discs.

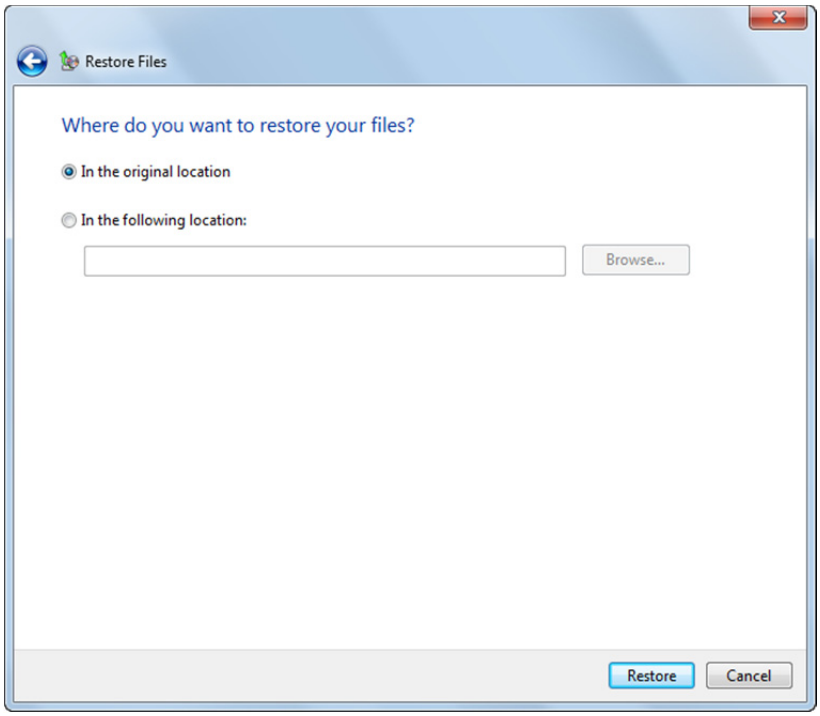
In this exercise, you set up and ran the Windows Backup utility.

## Restoring Files

In the event of a disk failure, or accidental deletion or other damage that has made one or more files non-recoverable, you can restore data to a hard drive from the saved backup media. To restore files, open the Backup and Restore window. Click the **Restore my files** button to open the Restore Files window.




To browse the contents of the backup media, click the **Browse for files** button or the **Browse for folders** button. (If you want to view individual files, use the Browse for files button). You can select specific files that you want to restore, or you can choose to restore all the files by selecting the highest level folder. After you have selected the files and/or folders, click **Next**.




You can restore files to their original location, or you can specify a different location. Specify the location, then click the **Restore** button. Windows restores the files to the specified location. Click the **Finish** button to close the Restore Files window, then close the Backup and Restore window of the Control Panel.

You can also use the Backup and Restore utility to create system images.

# System Images

A system image is an exact image of a hard drive; it includes Windows and your system settings, programs, and files. You can use a system image to restore the contents of a computer if the hard drive fails or the computer stops working. When you restore a computer from a system image, it is a complete restoration; you cannot choose individual items to restore, and all your current programs, system settings, and files are replaced.

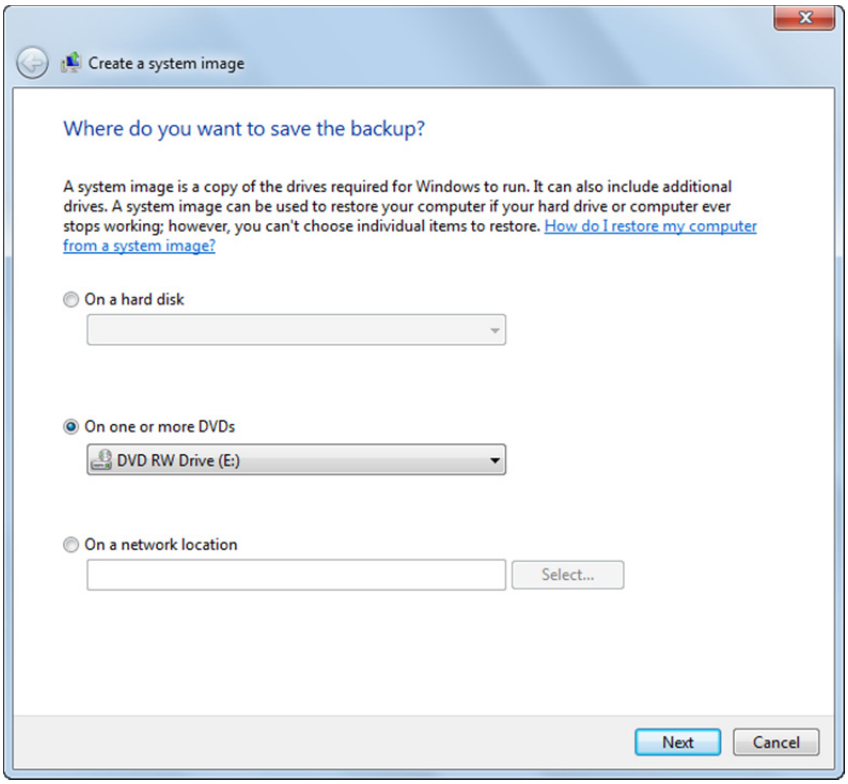
System images use the virtual hard disk (VHD) format used by Hyper-V and Windows Virtual PC. You can create a system image after installing Windows and other important applications and then easily revert to that state at any time in the future.

You create system images with the Backup and Restore utility.

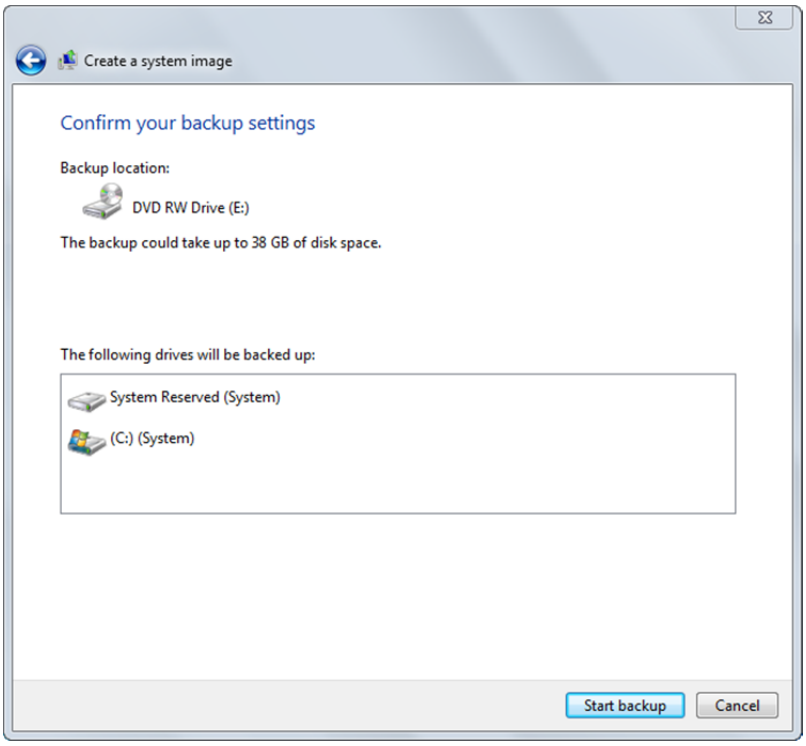
You can also use the Backup and Restore utility to create a system repair disk, which allows you to boot the computer if it becomes unbootable, and then restore the computer from a system image backup. The system repair disk is a bootable CD or DVD disk with the Windows Preinstallation Environment installed.

To create a system image:

1. Log on as an administrator.
2. Open the Backup and Restore window.
3. In the left pane, select **Create a system image**.




4. Choose the destination for the system image (a hard disk, one or more DVDs, or a network location) and click **Next**.




5. On the Confirm your backup settings screen, verify that the proper drives are listed for backup and click **Start backup**.
6. A screen will appear, telling you that Windows is saving the backup. Depending on the size of the backup the process can take from several minutes to more than an hour. You can click Stop Backup at any time to cancel the backup.
7. When the backup completes, you may be asked to create a System Repair Disk.
8. Click **Close** when you see a screen indicating the system image has been created.

## System Protection (Restore Points)

System Protection is a feature that enables you to re-establish the computer's system files to their state at an earlier point in time. It provides a way to undo changes without affecting personal files, such as documents or email.

System Protection works by regularly creating and saving information about a computer's system files and settings. It also saves previous versions of files that you have modified. System Protection saves this information in restore points, which are created just before significant system events, such as the installation of a program or device driver. Restore points are also created every seven days if no other restore points were created in the previous seven days. You can also create restore points manually at any time.

A *restore point* is a component of Windows ME, XP, Vista and Windows 7 that allows you to roll back system files, registry keys and installed programs to a previous state. Restore points can be extremely helpful if a system begins to malfunction after upgrading or updating software or making a configuration change. You can think of a restore point as a saved "snapshot" of a computer's data and settings at a specific point in time.

Restore points store information about registry settings, device drivers, configurations, etc. Restore points are managed by the System Protection utility, which monitors the system for important changes such as the installation of updates or new software. The utility saves settings and backup files for each restore point it creates.

The following information is included in a restore point:

- System files
- Registry settings
- Executable files
- Script files
- Batch files
- Shadow copies of user data files (copies of the files retained on the system for recoverability purposes)

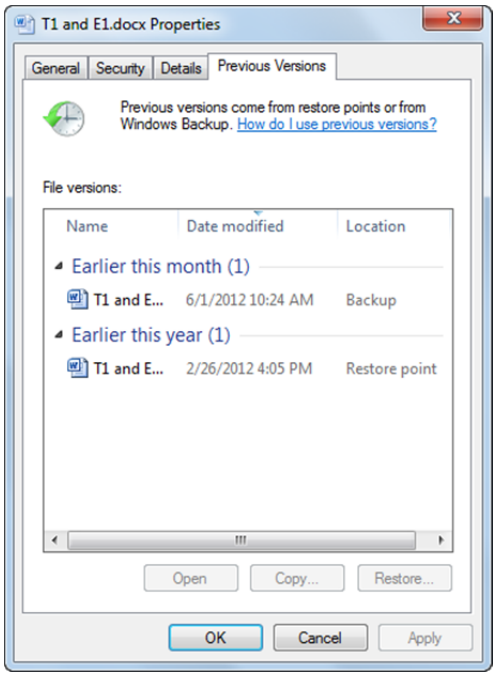
If your computer is running slowly or is not working properly, you can revert the computer to its previous settings using a restore point. Reverting to a restore point restores system settings, installed programs and drivers. However, reverting to a restore point does not affect personal files and settings. Reverting to a restore point will not recover a data file or your browsing history, for example.

If you accidentally modify or delete a file or folder, you can restore it to a previous version that has been saved as part of a restore point.

## Previous Versions

Previous versions are copies of files and folders that Windows automatically saves as part of system protection. You can use previous versions to restore files or folders that you accidentally modified or deleted, or that were damaged. If system protection is turned on, Windows automatically creates previous versions of files and folders that have been modified since the last restore point was made. Typically, restore points are made once a day. If your disk is partitioned or if you have more than one hard disk on the system, you need to turn on system protection for the other partitions or disks. Previous versions are also created by Windows Backup when you back up your files.

To restore a file or folder to a previous version, navigate to the file in Windows Explorer, right-click it and then select **Restore previous versions** in the shortcut menu. Windows will display the previous file versions.




It is important to understand that when you restore a previous version, the file or folder will replace the current version on your computer, and the replacement cannot be undone. Before restoring a previous version, select a version in the dialog box, and then click **Open** to view it and make sure that it is the version you want.

Note that you cannot open or copy previous versions of files that were created by Windows Backup, but you can restore them. To restore a previous version, select it in the dialog box, then click **Restore**.

If the Restore button is not available, you cannot restore a previous version of the file or folder to its original location. However, you might be able to open it or save it to a different location.

## Working with Restore Points

System Protection must be enabled on a drive in order for restore points to be created. It is automatically enabled for the System drive; however, you can enable system protection on other drives as well as long as the drives are formatted with the NTFS file system. In addition, the drive must be at least a 1 GB drive with 300 MB of free space. As disk space gets lower on a system, older snapshots or restore points will automatically be deleted to make room for new ones. You can also manually delete existing restore points or delete them using the Disk Cleanup utility.

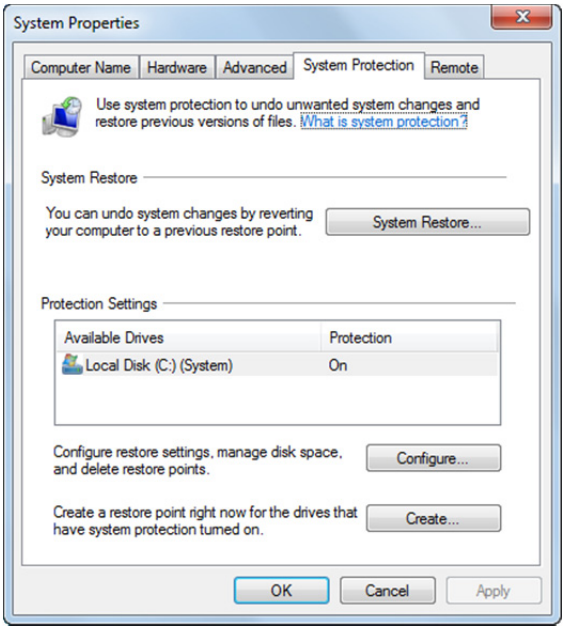
You can enable system protection for both system settings and previous versions of files or only for the restoration of previous versions of files. You can also indicate the maximum space it can use.

# Exercise 6-4: Working with System Restore

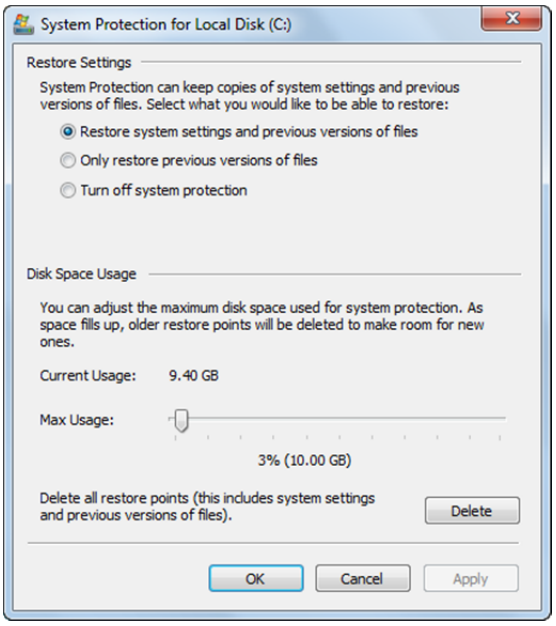

You can use system protection settings to create restore points; restore previous versions of files; allocate a specific amount of disk space for system restore files; and delete old restore points, settings and previous versions.

In this exercise, you will examine system protection settings and manually create a restore point.

1. Click **Start**, right-click **Computer** and select **Properties** to open the System window.
2. In the left pane of the window, click the **System protection** link to open the System Properties dialog box. The System Protection tab is active by default.



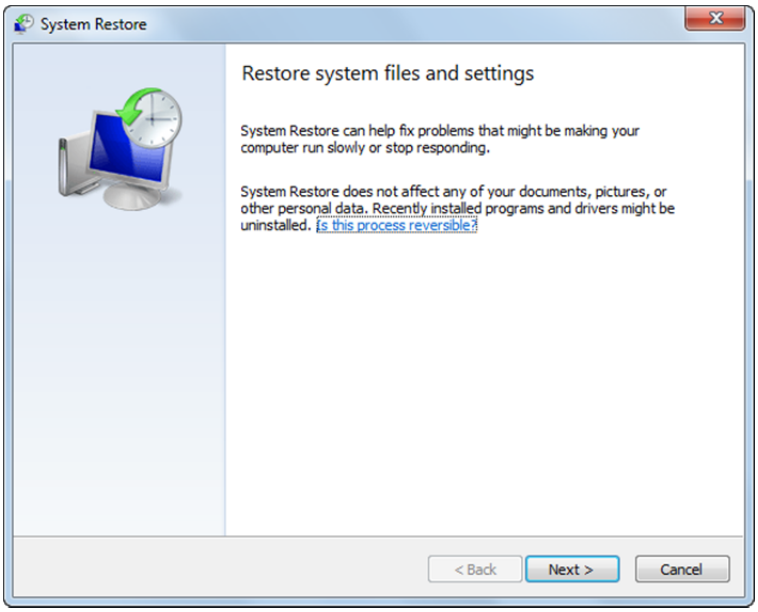

3. Click the **Configure** button.



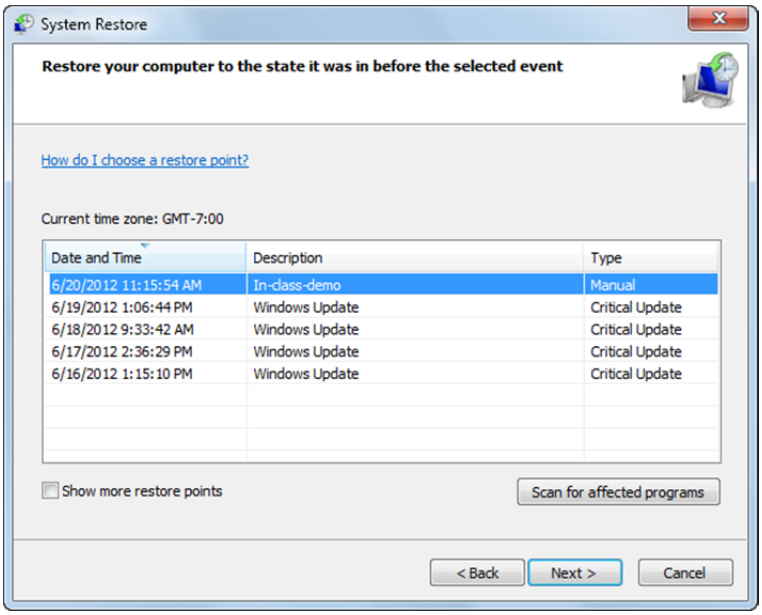

You can specify settings for each drive on which System Protection is turned on. In the Restore Settings section, you can control how much information Windows preserves. In the Disk Space Usage section, you can adjust the maximum amount of disk space allocated for system protection files. You can also delete all restore points, system settings and previous versions (except the very latest).

4. Click **Cancel** to close the System Protection dialog box.
5. In the System Protection tab of the System Properties dialog box, click the **Create** button to open the Create a restore point window, type a description to help you identify the restore point, then click the **Create** button.

   When Windows has finished creating the system restore point, the Restore point was created successfully window appears.
6. Click the **Close** button to close the notification window.
7. Click the **System Restore** button to open the Restore system files and settings window.



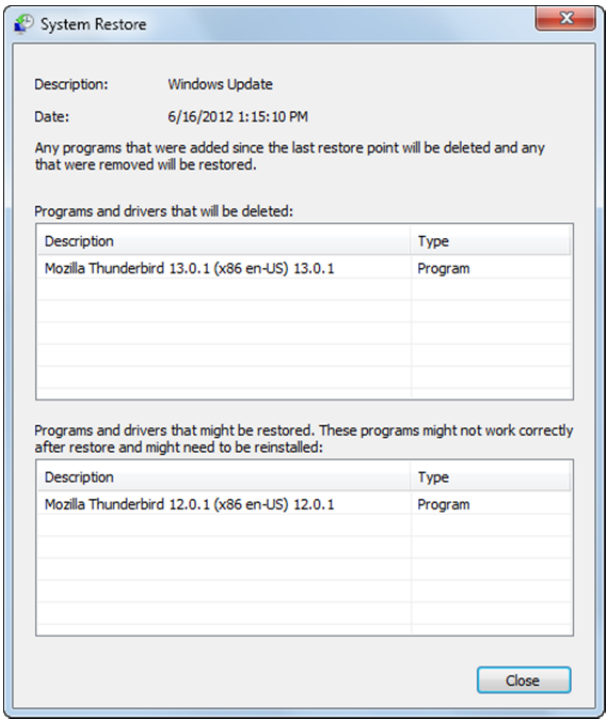

8. Click **Next** to view the available restore points.




Windows displays several restore points. Notice that the most recently created one appears at the top of the list. Notice also that Windows indicates a type for each restore point.

If your system does not display any restore points, select the **Show more restore points** check box.

9. Click the oldest restore point listed to select it, then click the **Scan for affected programs** button. Windows displays a list of any programs that would be affected if you rolled back the system to the selected restore point.




10. Click the **Close** button, click the **Cancel** button, then close any open dialog boxes.

In this exercise, you examined system protection settings and manually created a restore point.

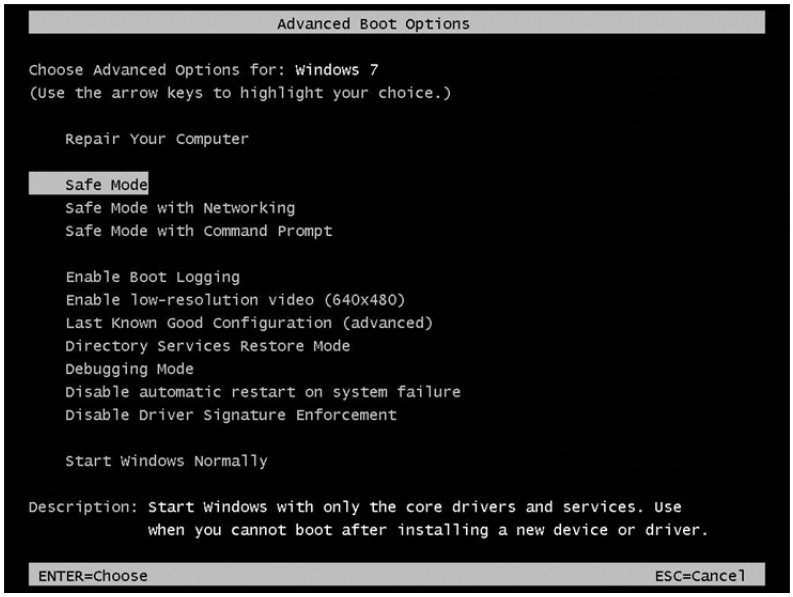
# Recovery Boot Options

Situations may arise where after installing updates or new device drivers, you will be unable to boot the system normally. In such cases, Windows starts to load, but then halts before displaying the Desktop.

In many disaster recovery cases, your system will not boot at all and you must use a system repair disk or the Windows 7 installation media just to boot into the Windows Recovery Environment. In other cases, you can use the advanced boot menu to access special boot-time options.

## Advanced Boot Options

The Advanced Boot Options menu is a list of advanced troubleshooting tools and Windows startup methods that can be used to repair files, start Windows with the minimum necessary processes, or restore previous settings. To access the Advanced Boot Options menu, press the F8 key continually after powering on the machine until the menu appears.




To start Windows in a particular mode, or to start a diagnostic tool, select one of the options and press ENTER. The Advanced Boot Menu provides the following options:

| | |
|---|---|
| **Repair Your Computer** | Displays a list of system recovery tools you can use to repair startup problems, run diagnostics or restore the system. |
| **Safe Mode** | Starts Windows with only the core drivers and services. Use this option when you cannot boot after installing a new drive or driver. |
| **Safe Mode with Networking** | Starts Windows with core drivers, plus networking support. |
| **Safe Mode with Command Prompt** | Starts Windows with core drivers, and launches the command prompt. |
| **Enable Boot Logging** | Creates a file called ntbtlog.txt, which lists all drivers that load during startup, including the last file to load before a failure. You can reference this log and determine which driver was last successfully loaded, and arrive at a starting point for troubleshooting. |
| **Enable low-resolution video (640x480)** | Starts Windows in low-resolution display mode. This option does not change the display driver, but is useful when the screen resolution has been changed to one that the monitor you're using does not support, thereby providing you an opportunity to start Windows at a universally accepted resolution so you can then configure the resolution at an appropriate setting. |
| **Last Known Good Configuration (advanced)** | Starts Windows with the drivers and registry data that were recorded the last time Windows was successfully started and then shut down. |
| **Directory Services Restore Mode** | Starts Windows in Directory Services Repair Mode, which repairs the directory service. This option applies only to Windows domain controllers. |

| | |
|---|---|
| **Debugging Mode** | Enables the Windows kernel debugger. This is an advanced diagnostic mode in which data about Windows is sent to a debugger. |
| **Disable automatic restart on system failure** | Prevents Windows from automatically rebooting after a serious system failure, such as a Blue Screen of Death. |
| **Disable Driver Signature Enforcement** | Allows unsigned drivers or drivers containing improper signatures to be loaded. |
| **Start Windows Normally** | Starts Windows using its regular settings. |

### Booting to Last Known Good Configuration

The Last Known Good Configuration option allows you to boot the computer with the hardware configuration that last allowed the system to start up and display the Desktop. This option can provide an easy fix for a problem due to a registry or driver change. For example, if you install a new video driver and then reboot the computer and start experiencing failures, you can boot with the Last Known Good configuration option and access the system with the old drivers.

If you boot a system after installing new hardware drivers and you notice that it is not acting normally before you log on, do not log on. Shut the computer down at the logon screen and then start it with the Last Known Good Configuration. If you log on, the current configuration becomes the Last Known Good Configuration because Windows assumes it is working properly or you wouldn't have been able to get to the Desktop.

### Using Safe Mode Options

Safe Mode is a special boot option that loads only core drivers and services. Within Safe Mode, however, you can usually back up any critical user files to a removable storage device such as a flash drive. You can also use Safe Mode to adjust some system settings and if necessary, to restore the system to one of the available restore points.

Sometimes when the system encounters problems, you may be given a menu option to boot into Safe Mode when you first power up the system. To force a system to boot into Safe Mode, you can press the F8 key continually as the system is powering up and then select **Safe Mode** from the Advanced Boot Options menu.

There are three Safe Mode options in Windows 7. Generally, you would use Safe Mode when you cannot boot the system any other way; and it is often used after installing a new device or driver that is preventing the system from booting normally.

Safe Mode can also be used for troubleshooting when you think a driver or application may have become corrupted. The three options work as follows:

| | |
|---|---|
| **Safe Mode** | Boots the system with a minimal set of drivers and services. Networking will not be available. You can use this mode any time you are trying to reinstall network drivers or network software. |
| **Safe Mode with Networking** | Boots the system in the same manner as safe mode, but adds network drivers only. This mode is useful when you need to access the network for other drivers or software. |
| **Safe Mode with Command Prompt** | Boots the system in the same manner as safe mode, but does not load Explorer as the user interface; instead you can issue commands at the Windows command prompt. This mode is useful if you suspect that Explorer is corrupted. |

# Understanding Updates

Objective 6.3

All operating systems and applications are vulnerable to attack as hackers and malware creators discover new weaknesses. For this reason, vendors continually release updates in various general forms.

A *patch* is a file of programming code that is inserted into an existing executable program to fix a known problem, or bug. Patches are designed to provide an immediate solution to a particular programming problem and can often be downloaded from the software vendor's website. However, patches are intended to be only temporary solutions until problems can be permanently repaired.

Generally, a software vendor will provide permanent solutions to program bugs in later product releases, known as updates. An *update* is any file or collection of software tools that resolves system liabilities and improves software performance. Updates are released periodically when deemed necessary by the vendor. A major update with significant software improvements may be marketed as a new release.

A *service pack* is a collection of updates, and is typically released after enough updates have accumulated to warrant the release. Service packs typically contain all previous updates, which include security patches, bug fixes, new features, utilities and applications.

## Microsoft Update Types

Microsoft provides periodic software updates. Every Microsoft product group includes an engineering team that is responsible for developing updates in order to resolve problems. The update process is as follows:

1. Microsoft is made aware of a security vulnerability or other problem.
2. The issue is escalated and verify by the Microsoft Security Response Center.
3. The product groups engineering team creates and tests an update.
4. Microsoft distributes the update through the Microsoft Download Center and other services.

Microsoft updates are released in the forms described in the following table.

| | |
|---|---|
| **Security Update** | A broadly released fix for a specific product, addressing a security vulnerability. A severity level is associated with a security update. The severity can be minimal or critical. |
| **Critical Update** | A broadly released fix for a specific problem, addressing a critical, non-security related bug. |
| **Update** | A broadly released fix for a specific problem, addressing a non-critical, non-security related bug. |
| **Hotfix** | A single package composed of one or more files used to address a problem in a product. Hotfixes address a specific customer situation, and are available only through a support relationship with Microsoft. Hotfixes may not be distributed outside the customer organization without written legal consent from Microsoft. |
| **Service Pack** | A cumulative set of hotfixes, security updates, critical updates, and updates since the release of the product, including many resolved problems that have not been made available through any other software updates. Service packs also may contain a limited number of customer-requested design changes or features. Service packs are broadly distributed and tested by Microsoft. |

## Installing Application/Operating System Updates as Required

While operating systems and applications must be updated to remain secure, not all updates are necessary, and at times, updates cause unexpected conflicts and even failures. For this reason, application and operating system updates should be evaluated before being installed, especially if corporate systems must interact with old hardware or old applications and compatibility may become an issue.

Many security policies require an extensive testing process before an update is installed onto any production system. If the patches or updates do not address the problems your system is experiencing, or if there would be no performance gain by applying them, you should not install them. Patches and updates can cause incompatibility problems among system resources or applications, and can even introduce new security issues. However, if your system is vulnerable to a security problem, you may need to install the patches or updates as soon as possible.

You should always ensure that you use stable updates which originate from a trusted source (such as the vendor that sells the product). Always verify that updates are, in fact, updates, and not Trojans. Always check for a valid digital signature and check the files with antivirus software.

## Windows Update

Windows Update is a service provided by Microsoft that provides updates for the Microsoft Windows operating system and its installed components, including Internet Explorer.

In Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 you use the Control Panel to configure update settings and check for updates. Updates are downloaded from the Windows Update website.

There are different kinds of updates. Security updates or critical updates protect against vulnerabilities to malware and security exploits. Other updates correct errors that aren't related to security, or enhance functionality.

Security updates are routinely provided on the second Tuesday of each month, but can be made available at any time when a new vulnerability is discovered. Other updates are not released on a regular schedule, only as the need arises. Windows Update can be configured to install critical updates automatically.

## Automatic Updating

You can configure Windows Update to automatically check for the latest updates. Depending on the settings you choose, Windows can install updates automatically or simply alert you that they are available. If you did not turn on automatic updating when you first set up the computer, you can still turn it on at any time.

If you don't use automatic updating, you should manually check for updates at least once every week. Microsoft typically releases important updates on the second or fourth Tuesday of the month. However, updates could be released at any time.

If you turned on automatic updating, then most security, reliability, and compatibility updates will be downloaded and installed automatically. Many updates, however, are not installed automatically; these include optional updates and updates that require you to accept new terms of use.

## Update Categories

Updates are categorized based on their importance. There are three categories for updates:

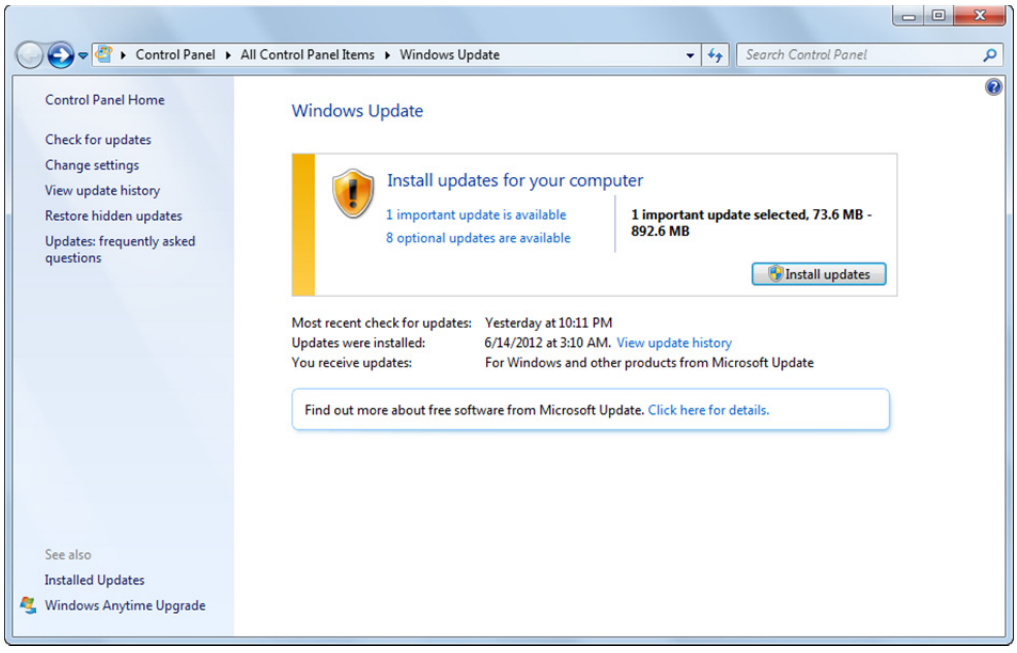
| | |
|---|---|
| **Important** | These updates include security and critical updates, as well as reliability improvements. |
| **Recommended** | These updates include software updates and new or improved features. If you selected **Use recommended settings** when you set up Windows Update, then recommended updates will be shown together with important updates. If you selected **Install important updates only**, recommended updates will be shown together with optional updates. |
| **Optional** | These updates include updates and software that you can install manually, such as new or trial Microsoft software or optional device drivers from Microsoft partners. |

## Microsoft Update

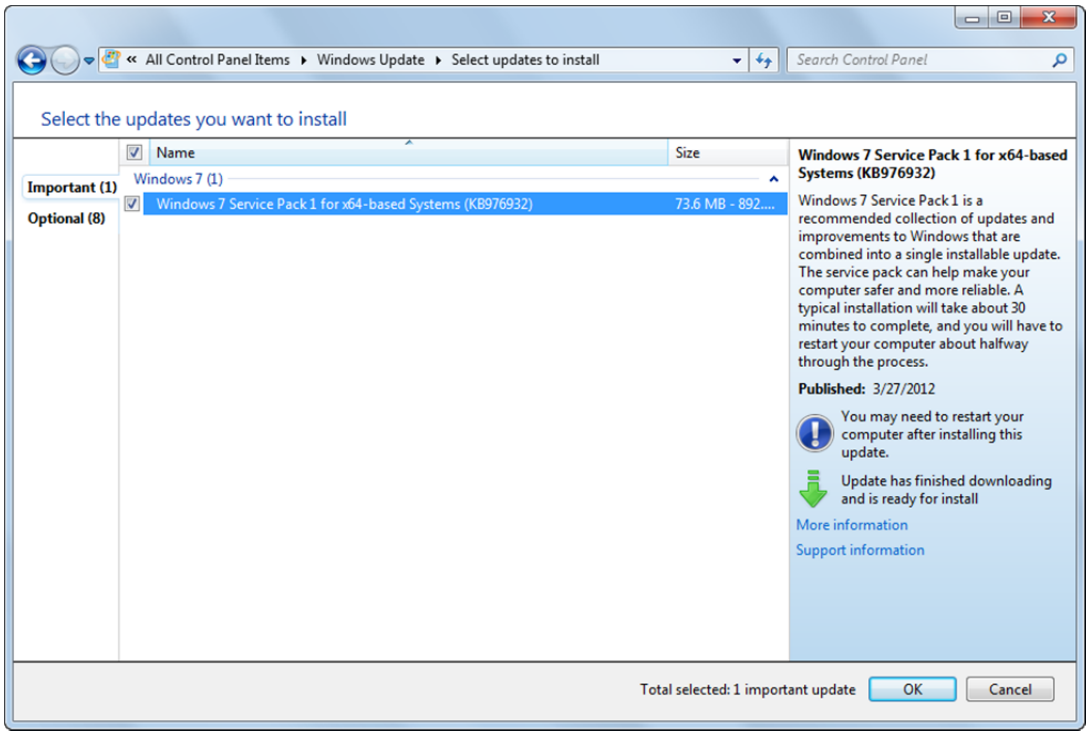
An optional feature enables access to Microsoft Update (instead of Windows Update). Microsoft Update is an expanded version of the update service which provides updates not just for the operating system and Internet Explorer, but also for other Microsoft software running under Windows, such as Microsoft Office, Windows Live applications, and Microsoft Expression Studio.

## Using Windows Update

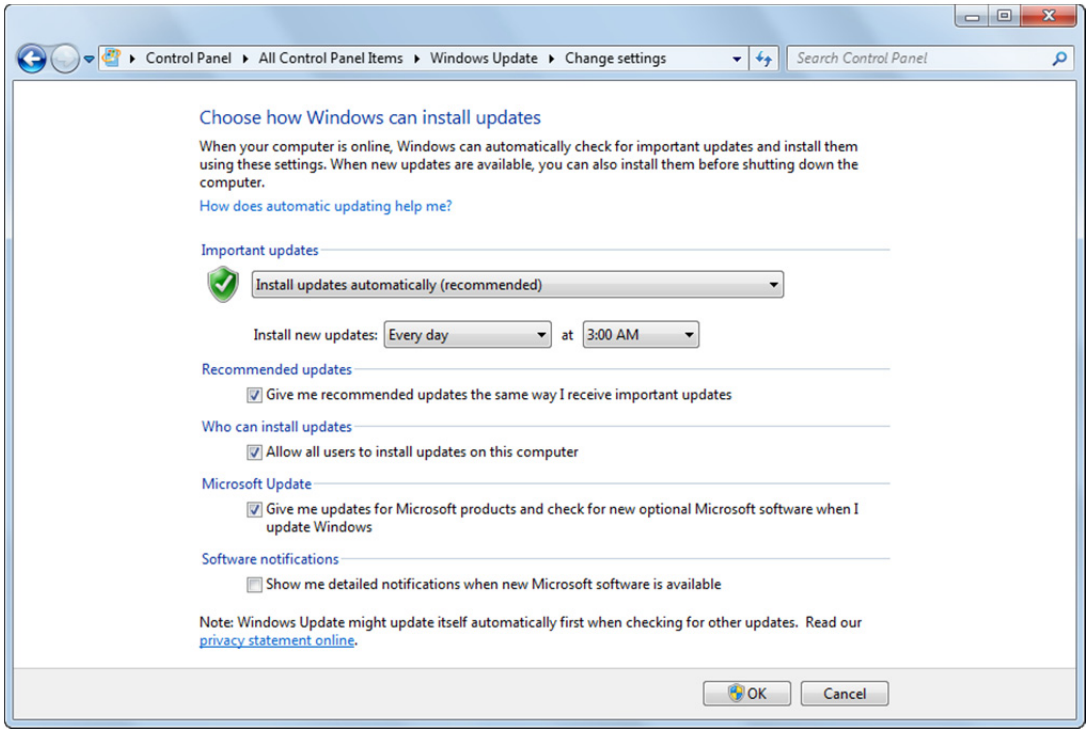
In Windows 7 and Windows Server 2008 R2, you access Windows Update through the Control Panel.



The Windows Update Control Panel shows the current status of available updates. You can click an update link to view details about the update.




From the Windows Update Control Panel, click the **Change settings** link to configure how updates are downloaded and installed.

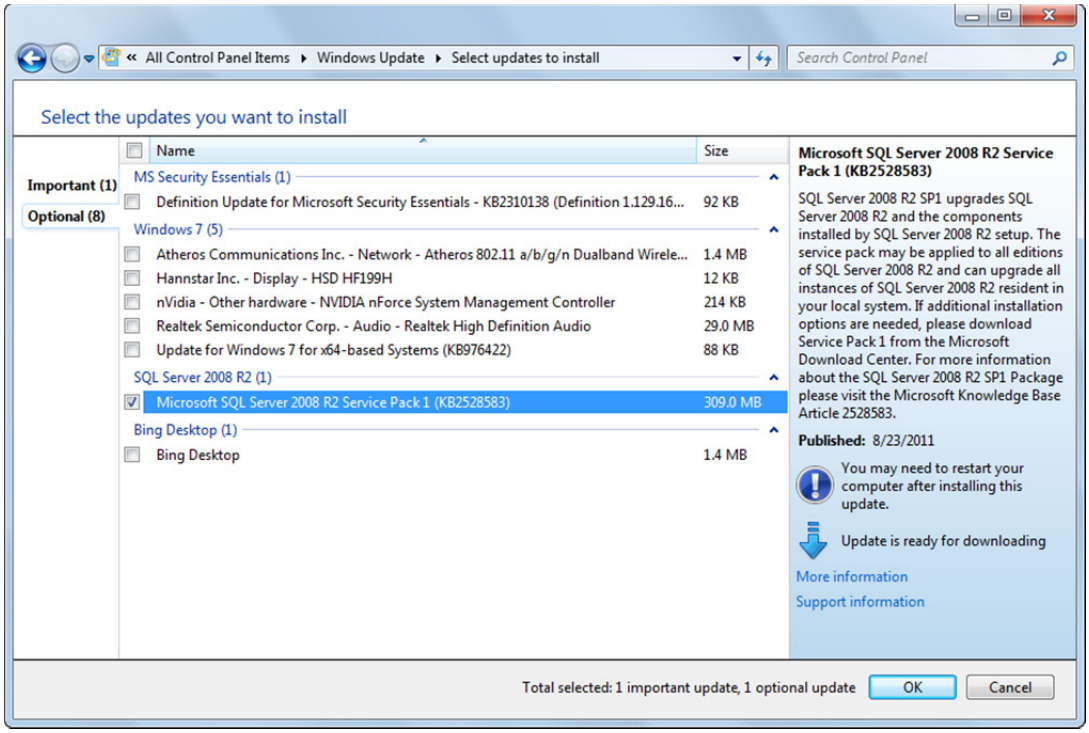


Notice that you can specify how important updates are downloaded and installed. The following options are available:

- Install updates automatically (recommended)
- Download updates but let me choose whether to install them
- Check for updates but let me choose whether to download and install them
- Never check for updates (not recommended)

You can also specify how recommended updates should be managed. By selecting the **Give me recommended updates the same way I receive important updates** check box, you are configuring Windows Update to automatically download (and possibly install, depending on the setting) recommended updates at the same time as important updates.

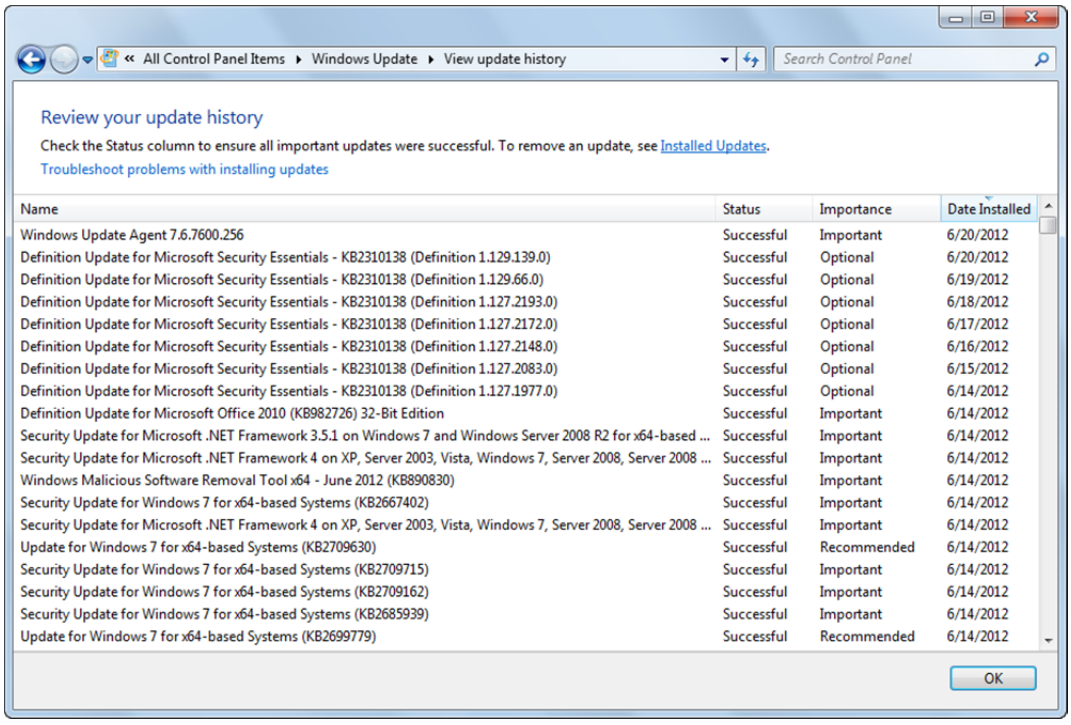
Optional updates are not downloaded or installed automatically. You can, however, manually install optional updates. Click the link for the available optional updates shown in the Windows Update Control Panel to view the details. Click the name of any update to view specific information about the update. Select the check box for any update you want to manually install.




Click **OK** to save your selections and return to the Windows Update Control Panel. Click the **Install updates** button to install the selected updates immediately. After updates are installed, you may be prompted to restart the system.

By selecting the **Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows** check box, you are configuring the update service to use Microsoft Update.

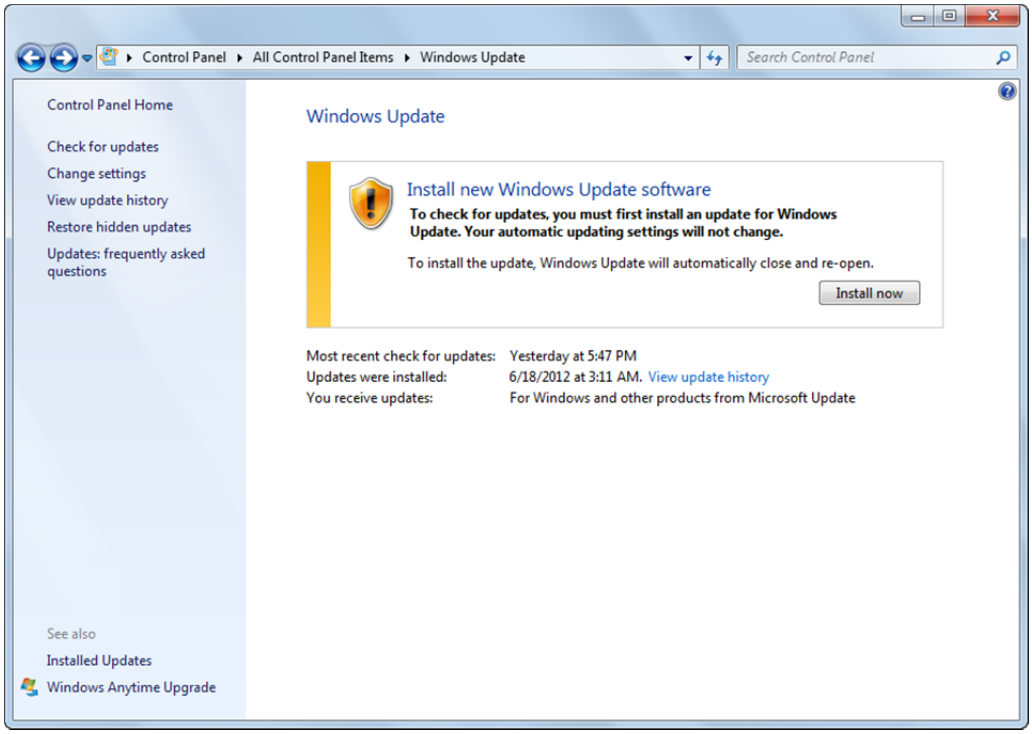
From the Windows Update Control Panel, you can click the **View update history** link to view a history of when updates have been installed.




From the Windows Update Control Panel, you can also click the **Check for updates** link to manually check for updates.

## Updating Windows Update

From time to time, Microsoft updates the Windows Update tool and service, and you may be prompted to install revised update software.




To install new update software, click the **Install now** button and follow the prompts on the screen. Windows Update may automatically close and reopen.

## Exercise 6-5: Working with Windows Update


In this exercise, you will explore Windows Update settings and check for new updates.

1. Open the Control Panel, switch to either Large or Small icons view if necessary, then click the **Windows Update** link to open the Windows Update Control Panel.

   Are updates available right now? If so, what type? _____

   When was the most recent check for updates? _____

2. If optional updates are available, click the link to open the Select updates to install page. Click one or two of the optional updates (do not select the check box) to view details about them.
3. Click the **Back** button to return to the Windows Update Control Panel.
4. In the left panel, click the **Change settings** link to view the current Windows Update settings. How is the system configured to handle important updates? _____

   When are updates scheduled to be installed? _____

   What other options are available for handling important updates? _____

   Do you think the current option is suitable for a client system? _____

   Would you use the same option for a server system? _____

   How are recommended updates handled? _____
5. Click the **Back** button, then click the **Check for updates** link. Are any additional updates now listed as available?
6. Close the Control Panel without installing any updates.

In this exercise, you viewed Windows Update settings and checked for updates.

### Windows Server Update Services

Windows Server Update Services (WSUS) is used to centrally manage updates and specify the ones you want to deploy to client computers in an enterprise. It is designed to support large-scale deployments, but scales well to small organizations as well. WSUS supports clients from Windows 2000 Professional through Windows Server 2008 R2.

# Maintenance Tools

Objective 6.2

Windows 7 provides several built-in tools for system maintenance. These include the Disk Defragmenter and Disk Cleanup utilities, the Task Scheduler, Action Center, and System Information tools.

You explored the Action Center earlier in this lesson. Its role in system maintenance is much like its role in system security – it provides a central place to view alerts and take actions that can help keep the system maintained and performing well.

## Disk Maintenance Tools

Maintenance tools help you maintain your hard disk and data to ensure that your system operates at peak efficiency. These tools also help prevent hardware problems and data loss. The following sections will discuss the purposes and uses of various disk utilities.

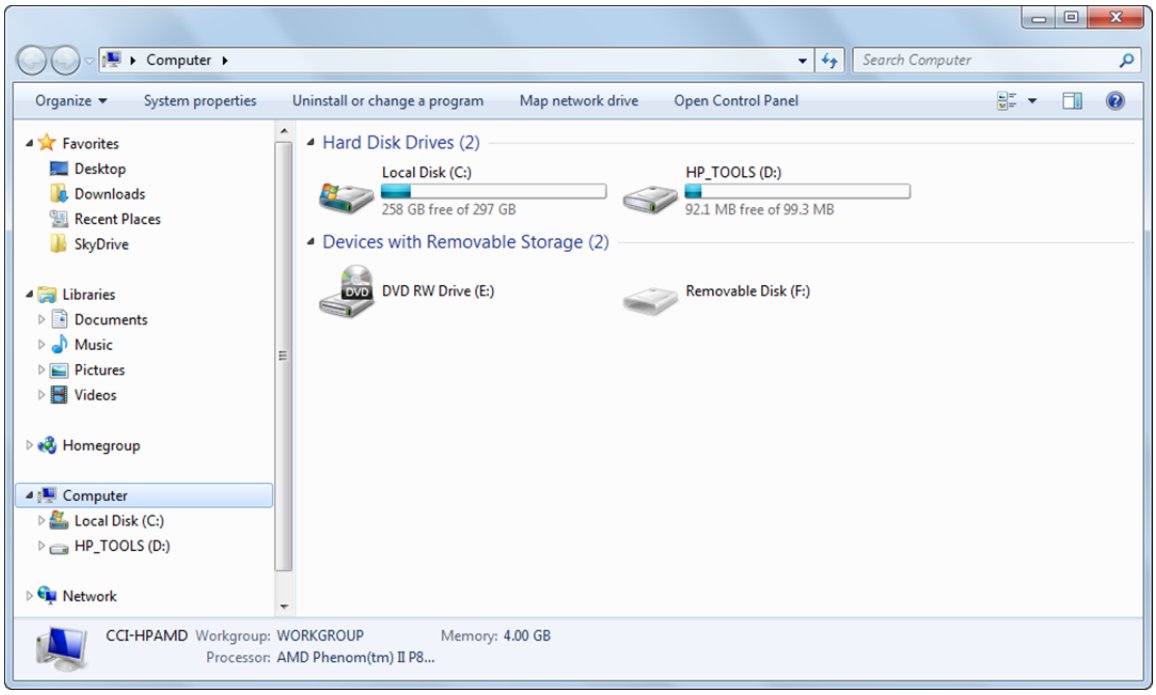
### Disk Defragmenter Utility

Over time, as files are created and deleted, a hard disk or disk partition can become severely fragmented. This means that individual files are not stored in contiguous sectors on the disk, but rather, they are scattered through various sectors on several regions of the disk. Fragmentation causes poor performance because the read/write heads have to jump from location to location to retrieve the file. The Disk Defragmenter utility defragments hard disks and puts fragmented files back together in a contiguous format.

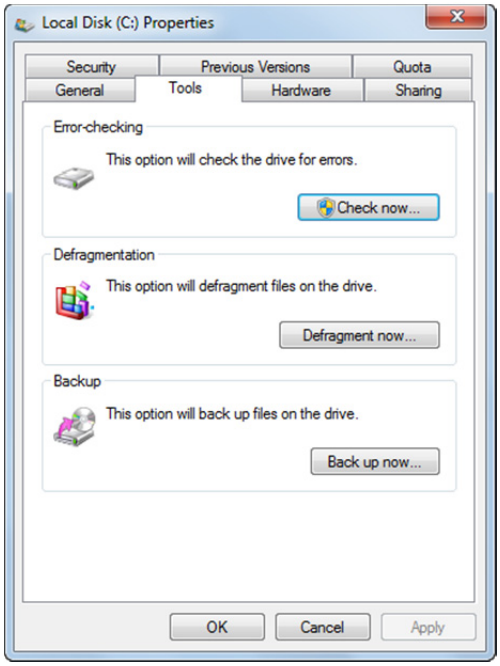
In previous versions of Windows, you had to periodically run the Disk Defragmenter tool. However, beginning with Windows Vista, the Disk Defragmenter runs automatically when the computer is idle. By default, Disk Defragmenter is scheduled to run every Wednesday at 1:00 a.m.

You can use the Task Scheduler to adjust the Disk Defragmenter schedule. (Task Scheduler is part of the Microsoft Management Console (MMC)). You can also configure the schedule from within the Disk Defragmenter dialog box.

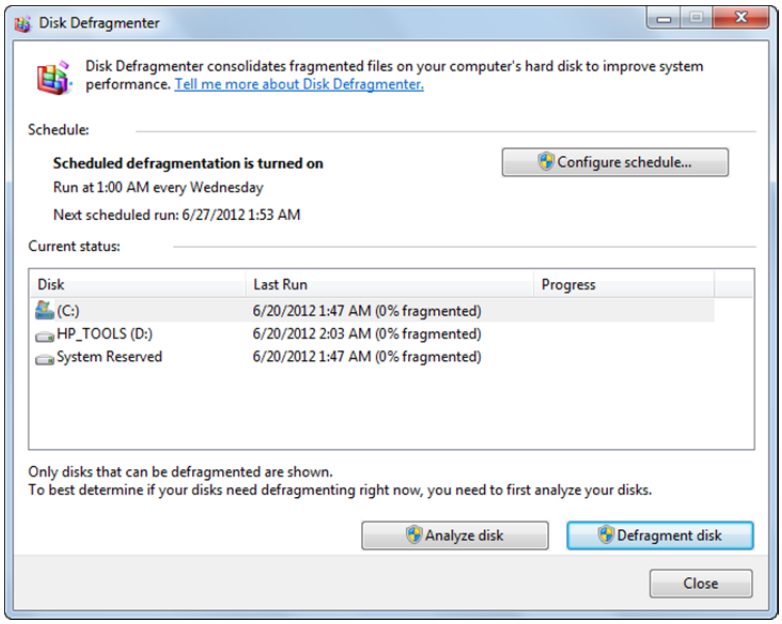
If you suspect that fragmented files are causing performance problems, you can start the Disk Defragmenter manually at any time. To run the Disk Defragmenter, click **Start**, then click **Computer** to open the Computer window.




In the Computer window, right-click a hard drive and select **Properties**, then click the **Tools** tab of the Properties dialog box.

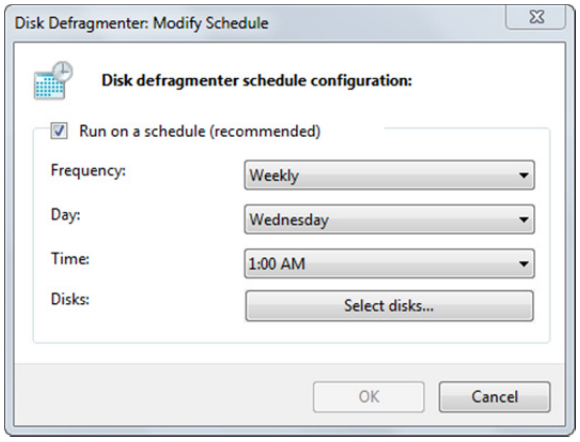



Click the **Defragment now** button to open the Disk Defragmenter dialog box, shown in the following figure. This dialog box shows the current schedule for Disk Defragmenter and shows the current fragmentation status of the various drives on the system.

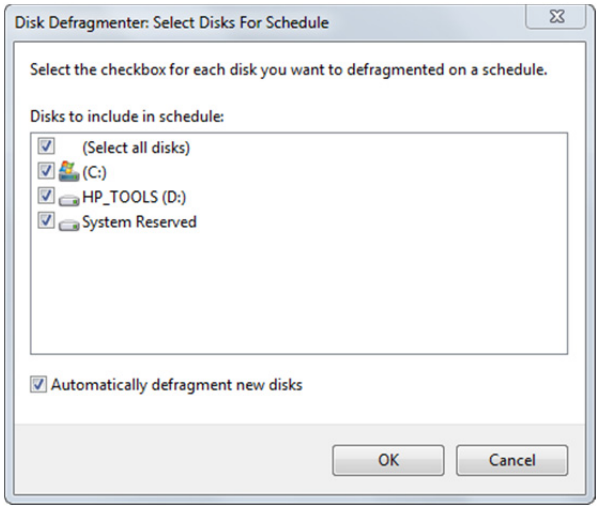



To analyze the hard disks, click the **Analyze disk** button. To run the Disk Defragmenter, click the **Defragment disk** button.

You can also change the schedule for defragmentation by clicking the **Configure schedule** button.




You can specify which disks to defragment by clicking the **Select disks** button.

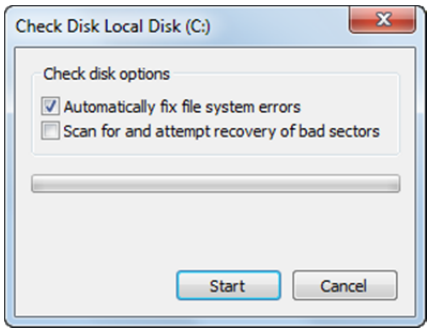


## Checking the Hard Disk for Errors

By periodically checking a hard disk for errors, you can prevent sudden hard disk problems. Sometimes errors occur when a program is writing information to a disk, or when the operating system is performing file management tasks (such as deleting, copying or moving files).

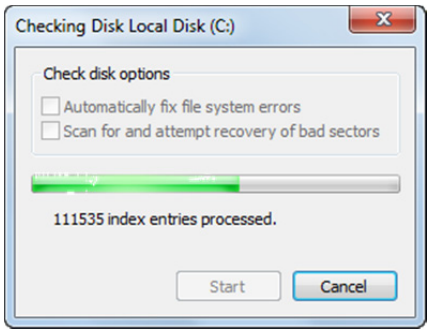
Windows uses the Check Disk (also referred to by its original name, *Chkdsk*) utility to examine a disk. The utility can automatically repair file system errors and can sometimes find and recover bad disk sectors.

To check the hard disk for errors, click **Start**, **Computer**, right-click a hard drive and select **Properties**, then click the **Tools** tab of the Properties dialog box and click the **Check now** button. The Check Disk dialog box will open and you can specify whether Windows should automatically fix file system errors and whether you want Windows to scan for and attempt to recover bad disk sectors.

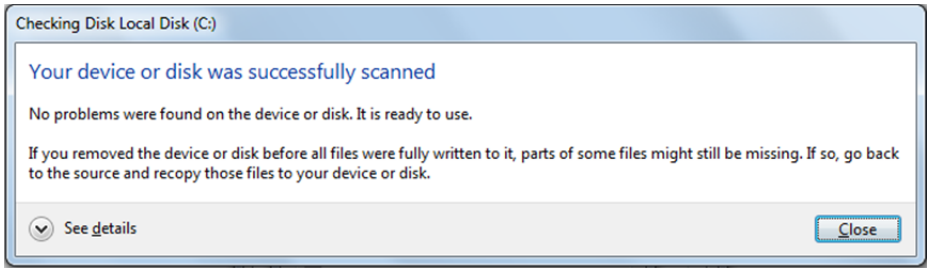



If you choose to have Windows fix file system errors automatically, the scan will be scheduled for the next time you restart the computer. If you clear the Automatically fix file system errors check box, then errors will be reported but not acted upon and the scan will begin as soon as you click the **Start** button.

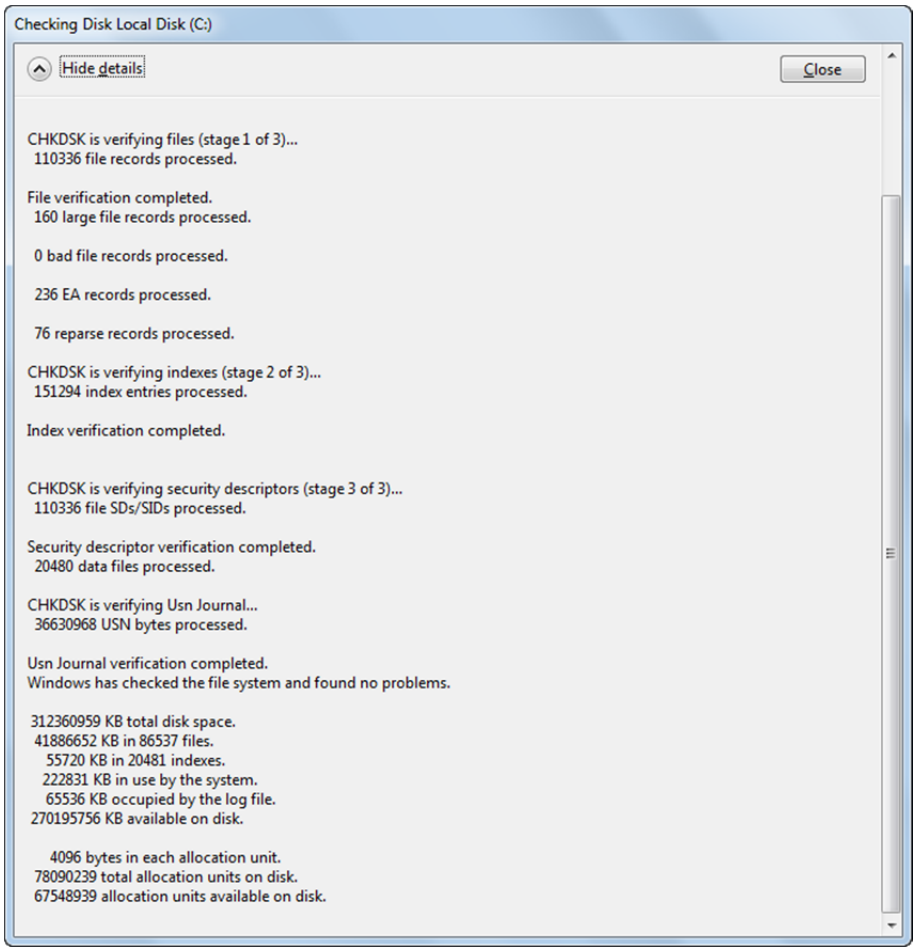
As a disk scan is underway, Windows shows a progress meter.




When the check is complete, Windows displays the results.




You can open the **See details** drop-down list to see the full results of the check disk utility.



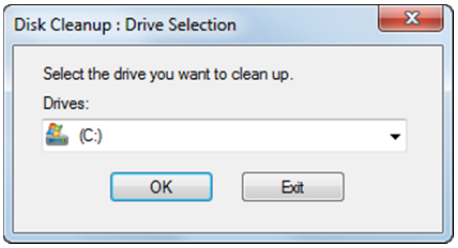

## Disk Cleanup Utility

Operating systems generate temporary files that you should periodically delete to conserve disk space. In some cases, deleting temporary files and directories will help you recover from application failures and from failed application installations.

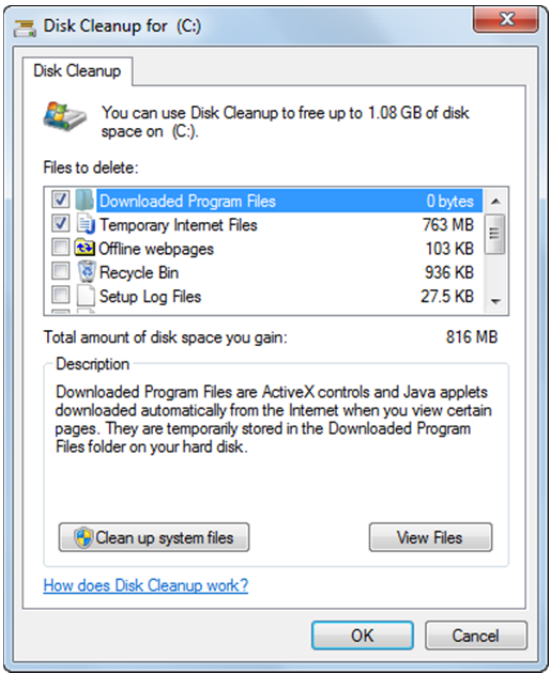
The Disk Cleanup utility enables you to recover the disk space used by temporary files, unused applications, files in the Recycle Bin, files you downloaded as part of web pages, and files created when the check disk utility attempts to recover lost file fragments.

Disk Cleanup scans your drive for files that can be safely deleted, but gives you the option to keep or delete them.

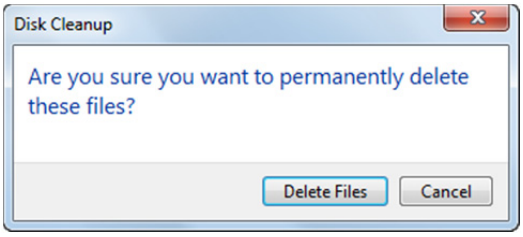
You can access the Disk Cleanup utility from the System Tools menu. Click **Start**, **All Programs**, **Accessories**, **System Tools**, **Disk Cleanup**. On a system that includes multiple hard drives, you begin by specifying which drive you want to clean up.



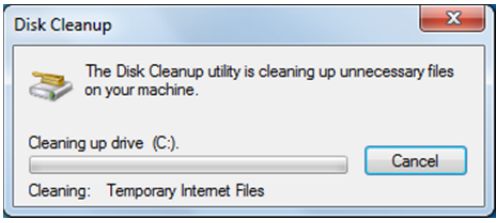
Click **OK** to allow the utility to analyze the selected drive. On a system that contains only one hard drive, the analyzing phase begins immediately without your needing to specify which drive to clean. When the analyzing phase is complete, the Disk Cleanup dialog box opens.




In the **Files to delete** list, select or clear the check boxes to specify which files you want to delete, then click the **OK** button. You are prompted to confirm that you want to delete the indicated files.




Click the **Delete Files** button to begin the cleanup process. Windows reports its progress.




The Disk Cleanup dialog box closes automatically when the process is complete.

## Task Scheduler

**MMM**
Scheduling Tasks

The Task Scheduler is a service that monitors for scheduled tasks and executes them at the defined time. Many tasks, such as the Disk Defragmentation task are built into the operating system. However, you can modify when and how these tasks are run using the Task Scheduler.

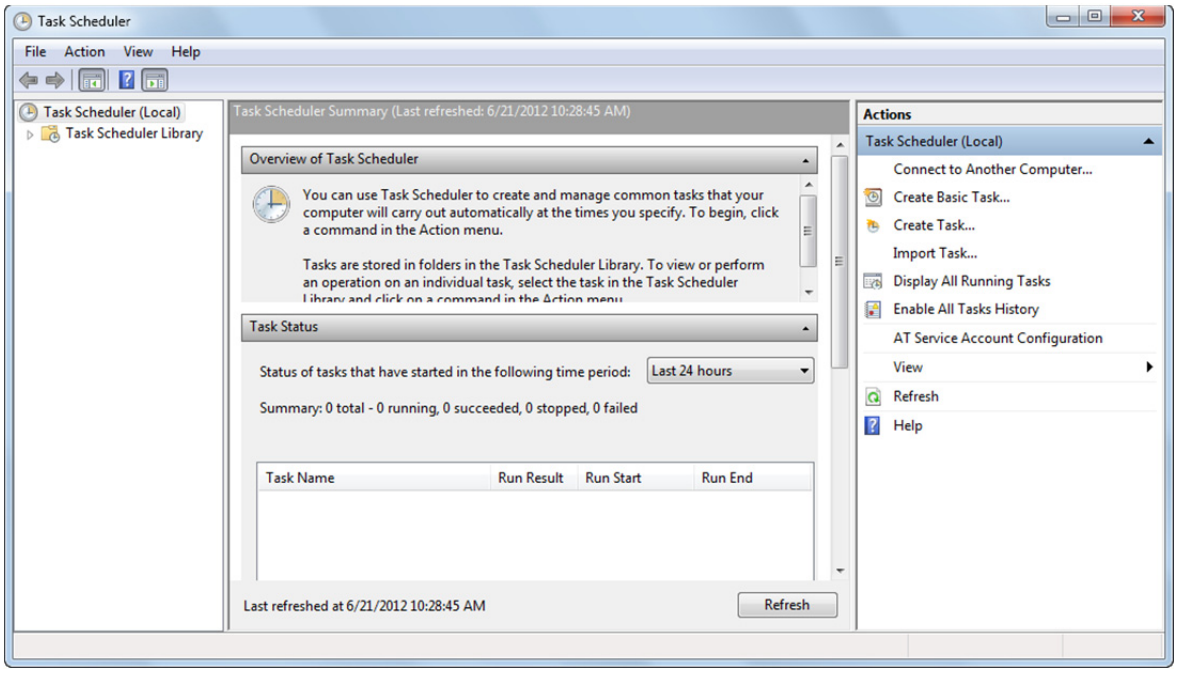
The Task Scheduler allows you to:

- Create scheduled tasks
- Display running tasks
- Import scheduled tasks exported from other computers

Tasks can run on a schedule or they can run based on triggers (occurrences or environmental conditions). The available triggers for the Task Scheduler are:

- System startup
- User logon
- System idle
- Creation of an Event Log entry
- Workstation locked
- Workstation unlocked

To open the Tasks Scheduler, click **Start**, **All Programs**, **Accessories**, **System Tools**, **Task Scheduler**. The Task Scheduler is shown in the following figure.



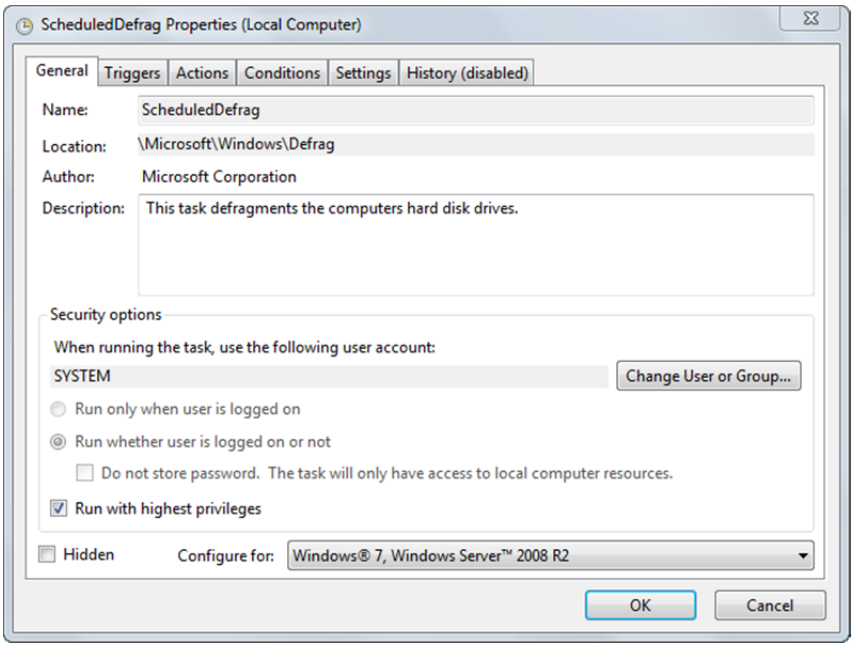

Tasks are stored in folders in the Task Scheduler library. To view or perform an operation on an individual task, select the task in the Task Scheduler library and click on a command in the Action menu.

## Exercise 6-6: Using the Task Scheduler

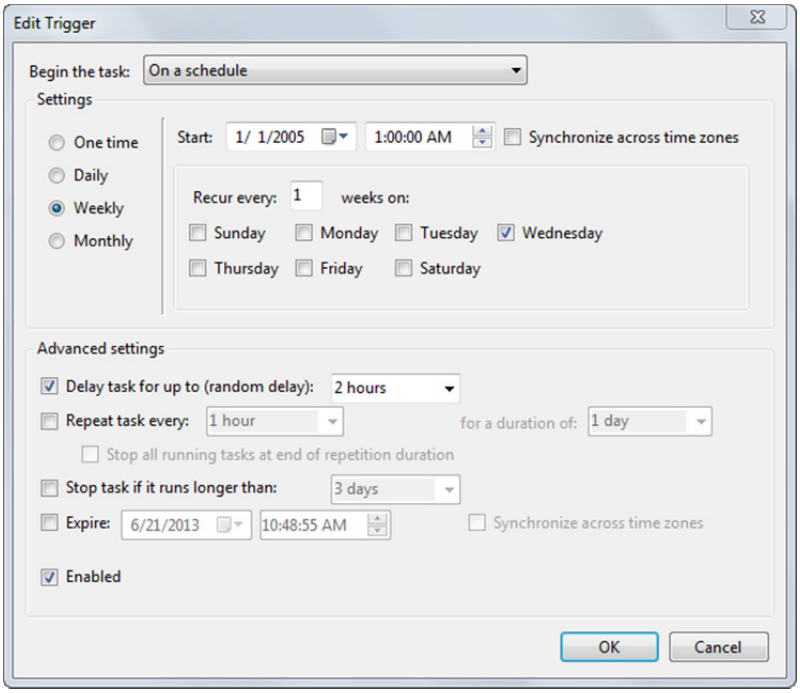

In this exercise, you will examine task properties, and create, test and delete a new task.

1. Click the **Start** button, click **All Programs**, click **Acces sories**, click **System Tools**, then click **Task Scheduler** to open the Task Scheduler.
2. In the left pane, expand the **Task Scheduler Library**, expand the **Microsoft** folder, expand the **Windows** folder, then click **Defrag** to select the Defrag task.

   Notice the options in the right pane. You can run the tasks immediately, end the task if it is running, disable it, export the task, examine its properties, or delete it.
3. In the middle pane, ensure that the **General** tab is selected, then scroll down if necessary to view which account this service uses when it runs. Which account does the Defrag task use?_____
4. Click the **Triggers** tab. When is this task scheduled to run? _____
5. Click the **Conditions** tab. Notice that you can specify under which particular conditions the task will run.
6. In the right pane, click **Properties** to open a Properties dialog box for the Defrag task. From here, you can edit the settings for the task.



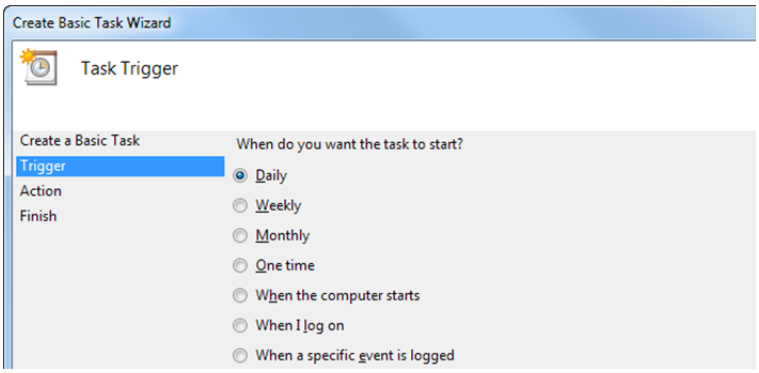

7. Click the **Triggers** tab in the dialog box, then click the **Edit** button to open the Edit Trigger dialog box. Notice that you can change the day, time and frequency with which the Defrag task is executed.



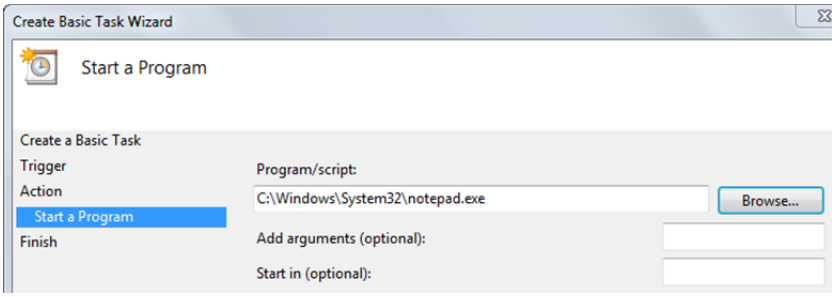

8. Click **Cancel** twice.

You can create a new task using the Basic Task wizard.

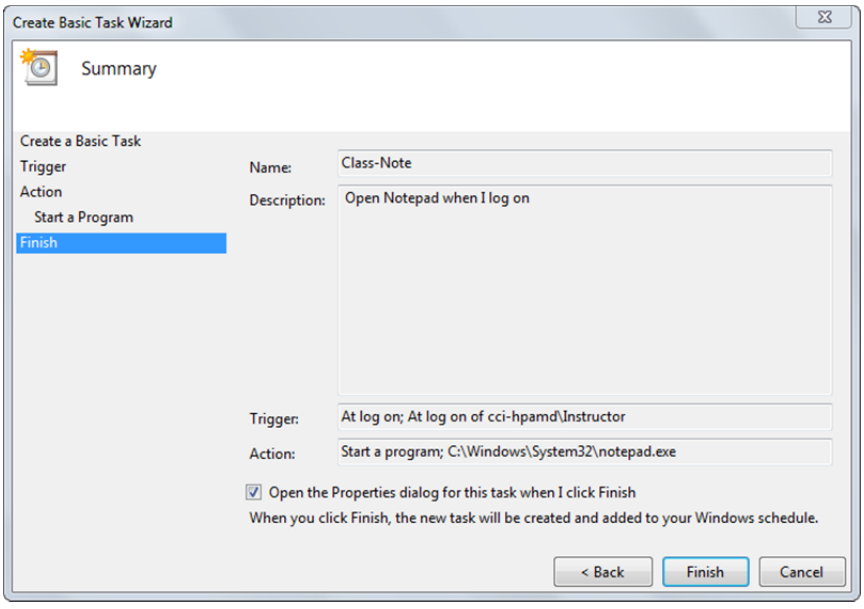
9. In the left pane, click **Task Scheduler (Local)**.
10. In the right pane, click **Create Basic Task** to start the Create Basic Task Wizard.
11. In the name box, type: `Class-Note`, press TAB, in the description box, type: `Open Notepad when I log on then` click **Next**.




12. In the When do you want the task to start column, select **When I log on**, to specify the logon event as the trigger for the task, then click **Next**.
13. Ensure that **Start a program** is selected for the action, then click **Next**.
14. Click the **Browse** button, navigate to the **C:\Windows\System32** folder, scroll the list, click **Notepad.exe**, then click **Open** to specify the path and application name.




15. Click **Next**.
16. Select the **Open the Properties dialog box for this task when I click Finish** check box.




17. Click **Finish**. Task Scheduler creates the task, adds it to the Windows schedule, and opens the Properties dialog box for the Class-Note task.
18. Examine the tabs in the Properties dialog box to familiarize yourself with the task settings. When you are done, click **OK**.

19. Close the Task Scheduler.

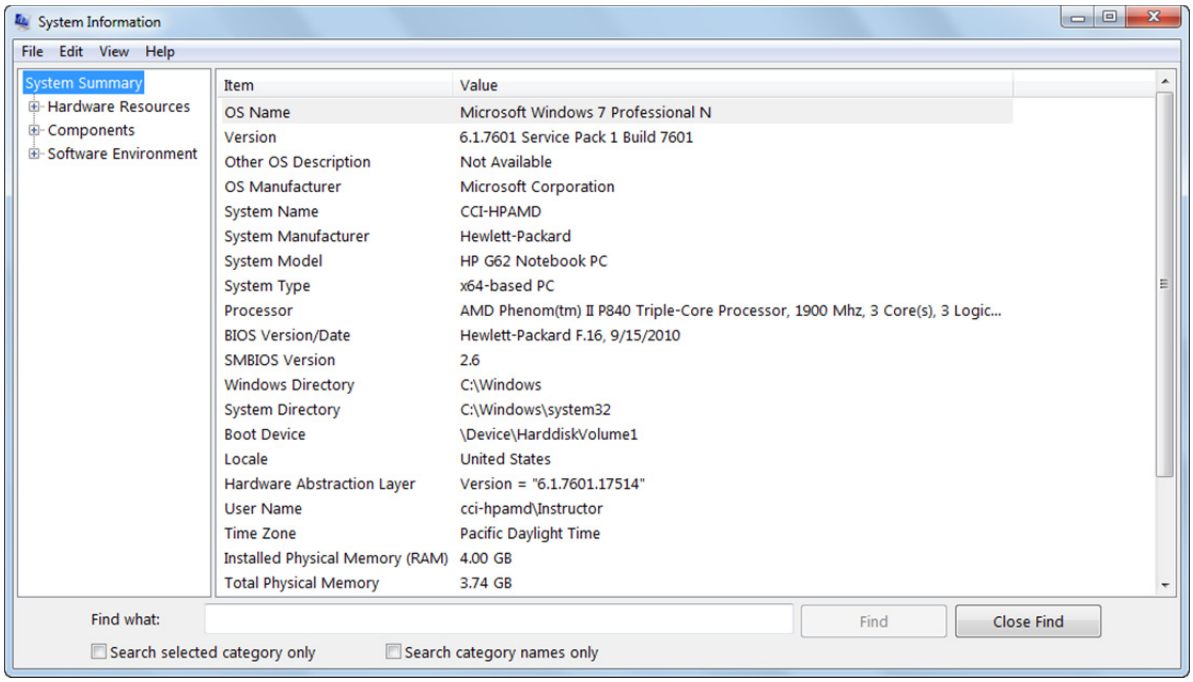
Now you can test your new task.

20. Click **Start**, point to the arrow next to Shut down, then select **Log off** to log off the system.
21. Log back on to the system. When you log back on, Notepad opens.
22. Close the Notepad window.
23. Open the Task Scheduler.
24. In the left pane, click **Task Scheduler Library**, then in the middle pane, click the **Class-Note** task.
25. In the right pane, click **Delete**, click **Yes** to confirm the deletion, then close the Task Scheduler.

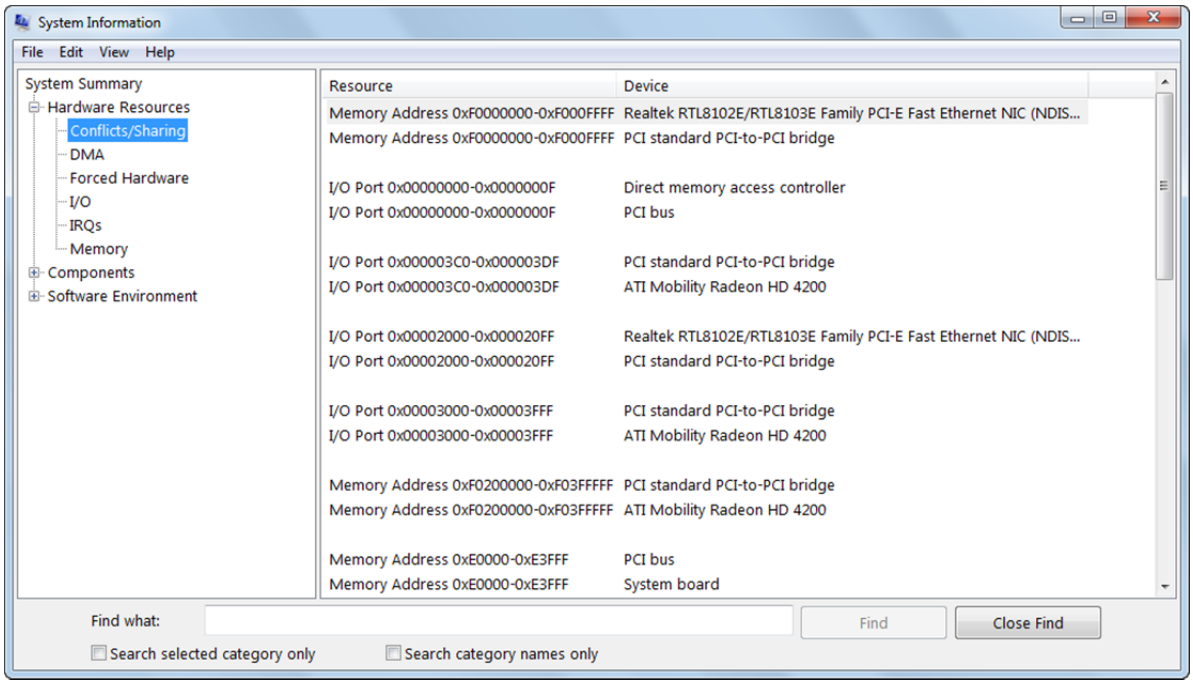
In this exercise, you examined task properties, and created, tested, and deleted a new task.

## System Information

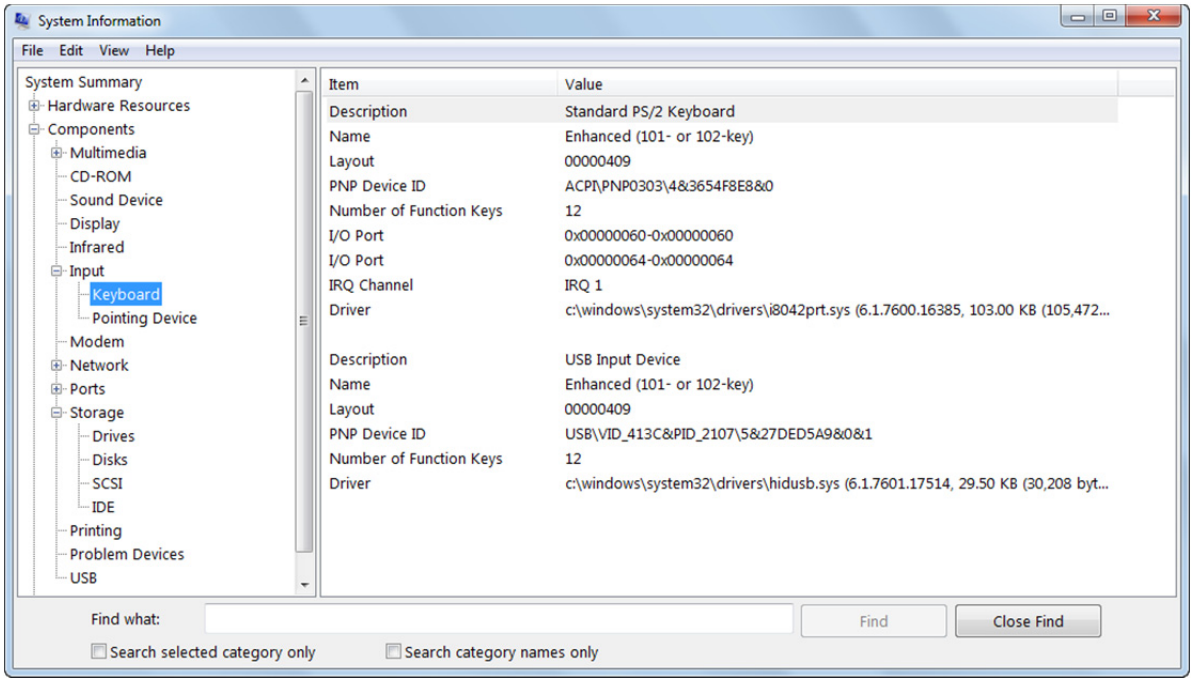
System Information is a graphical tool for viewing system configuration settings and properties. To open System Information, click **Start**, **Accessories**, **System Tools**, **System Information**.



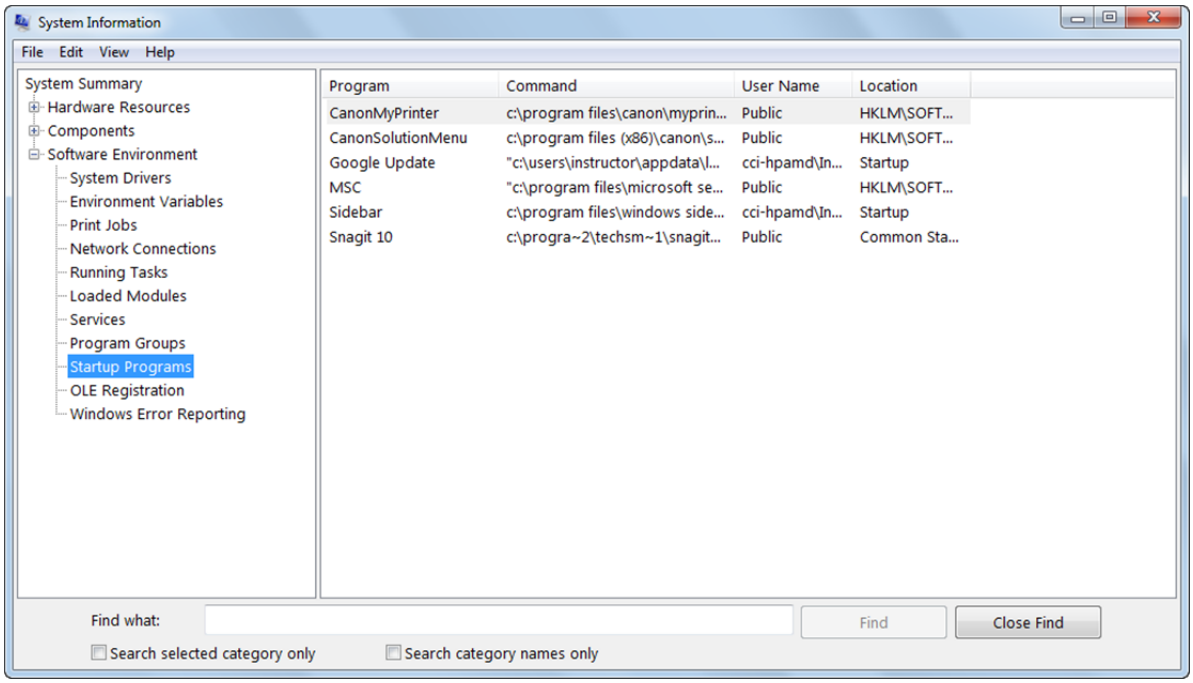

You can view information on hardware resources, such as conflicts, I/O addresses, IRQs, etc.




You can also view information on installed components, including input devices, network cards, sound devices, disks and drives, printers and USB devices.




You can also view information about the current software environment, including system drivers, print jobs, network connections, running tasks, services and startup programs.




# Lesson Summary

In this lesson, you learned about various tools and methods for maintaining a Windows 7 system. You are now able to:

- ☑ Identify various types of malware.
- ☑ Identify security risks other than malware.
- ☑ Explain how malware affects the Windows Registry.
- ☑ Explain the use of firewalls.
- ☑ Describe the function and purpose of antispyware software.
- ☑ Describe the function and purpose of antivirus software.
- ☑ Describe how to avoid malware infection.
- ☑ Understand the function of the Windows Action Center.
- ☑ Explain and use the Malicious Software Removal Tool.
- ☑ Describe and use Windows Defender.
- ☑ Describe the function of Microsoft Security Essentials.
- ☑ Describe the function of Microsoft Forefront Endpoint Protection.
- ☑ Explain Windows Backup and Restore.
- ☑ Describe the function of system images, restore points and previous versions.
- ☑ Explain Advanced Boot Options, including Safe Mode and Last Known Good Configuration.
- ☑ Describe Microsoft update types.
- ☑ Explain how to use Windows Updates.
- ☑ Explain and use Windows system maintenance tools, including Defrag and Disk Cleanup.
- ☑ Explain how to use the Task Scheduler.
- ☑ Describe the purpose and function of the System Information tool.

**MMM**
Go online for Additional Review and Case Scenarios

# Review Questions

1. Which of the following tools can you use to check the status of Windows Update, virus protection, and the firewall all in one place?
   a. The Action Center
   b. The System Information window
   c. The Task Scheduler
   d. The Disk Management snap-in

2. Which of the following antimalware tools must be downloaded from Microsoft before it can be used?
   a. Windows Defender
   b. The Malicious Software Removal Tool
   c. The Windows firewall
   d. The Windows Action Center

3. Which of the following tools can you use to restore a folder that you accidentally deleted?
   a. A system restore point
   b. The Disk Management snap-in
   c. Previous versions
   d. Safe Mode

4. Under which of the following conditions would you use the Last Known Good Configuration option?
   a. When Windows fails to boot successfully
   b. When you want to restore a file that was deleted
   c. When you want to roll back a driver to a previous state
   d. When you want to edit the Windows Registry

5. Which of the following tools can you use to stop the Defrag utility from running automatically?
   a. The Action Center
   b. The System Information window
   c. The advanced Boot Options menu
   d. Task Scheduler


# Appendices

## Appendix A: Courseware Mapping

## Appendix B: Glossary of Terms

## Appendix C: Index


# Courseware Mapping

| Exam 98-349<br>Windows Operating System Fundamentals | | |
|---|---|---|
| **Objective Domain** | **Topic Title** | **Lesson #** |
| **1. Understanding Operating System Configurations** | | |
| 1.1 Configure Control Panel options. | Configuring Control Panel Options | 2 |
| 1.2 Configure desktop settings. | Configuring Desktop Settings | 2 |
| 1.3 Understand native applications and tools. | Understanding Native Applications and Tools, Using the System Configuration Tool | 2 |
| 1.4 Understand mobility. | Understanding Mobility<br>Remote Desktop Connection | 2<br>3 |
| 1.5 Understand remote management and assistance. | Managing Remote Systems and Users | 3 |
| **2. Installing and Upgrading Client Systems** | | |
| 2.1 Identify Windows operating system editions. | Windows Operating System Versions and Editions | 1 |
| 2.2 Identify upgrade paths. | Understanding Windows Anytime Upgrade, Identifying Upgrade Paths | 1 |
| 2.3 Understand installation types. | Deployment Options | 1 |
| 2.4 Understand virtualized clients. | Introducing Virtualization<br>Remote Desktop Connection, Remote Desktop Services (RDS), Virtual Desktop Infrastructure | 1<br>3 |
| **3. Managing Applications** | | |
| 3.1 Understand application installations. | Installing and Uninstalling Applications, Group Policy | 3 |
| 3.2 Understand user account control (UAC). | User Accounts | 3 |
| 3.3 Remove malicious software. | Microsoft Malware Solutions | 6 |
| 3.4 Understand services. | Understanding Services | 3 |
| 3.5 Understand application virtualization. | MED-V<br>Application Virtualization, Virtual Desktop Infrastructure | 1<br>3 |
| **4. Managing Files and Folders** | | |
| 4.1 Understand file systems. | Understanding File Systems | 4 |
| 4.2 Understand file and print sharing. | Setting Up File and Print Sharing | 4 |
| 4.3 Understand encryption. | Understanding Encryption | 4 |
| 4.4 Understand libraries. | Working with Libraries | 1, 4 |

| | | |
|---|---|---|
| **5. Managing Devices** | | |
| 5.1 Connect devices. | Connecting Devices, Understanding Printing Devices | 5 |
| 5.2 Understand storage. | Understanding File Systems<br>Understanding Storage | 4<br>5 |
| 5.3 Understand printing devices. | Understanding Printer Devices | 5 |
| 5.4 Understand system devices. | Understanding System Devices | 5 |
| **6. Understanding Operating System Maintenance** | | |
| 6.1 Understand backup and recovery methods. | Windows Backup Methods and Tools | 6 |
| 6.2 Understand maintenance tools. | Microsoft Malware Solutions | 6 |
| 6.3 Understand updates. | Understanding Updates | 6 |


# Glossary of Terms

**adware** – a software application that automatically displays or downloads advertisements.

**antivirus applications** – applications designed to detect and eliminate viruses and other malware.

**application software** – software that is used to perform certain functions such as word processing or database functions.

**asymmetric-key encryption** – an encryption method which uses two keys, a public key and a private key. The public and private keys are mathematically related so only the public key can be used to encrypt messages, and only the corresponding private key can be used to decrypt them. Together, these keys are known as a key pair

**backup** – a duplicate copy of a program, a disk, or data, made either for archiving purposes or for safeguarding files from loss if the active copy is damaged or destroyed.

**bare metal (Type 1)** – hypervisor software that runs directly on top of the computer hardware without an operating system in between.

**clean install** – a method of installing Windows wherein the operating system files are installed fresh, user settings must be configured anew, user files and any programs that were installed on the system prior to the clean install must be reinstalled and reconfigured.

**client** – a system that requests a service or information from another computer on the network.

**cloud computing** – the practice of using applications or storage space on the Internet rather than on your own computers and servers. All that is required to use cloud computing services is a Web browser and an Internet connection; no other software needs to be installed.

**decryption** – the process of converting the encrypted data back to its original form.

**device** – any piece of equipment that can be attached to a network or computer, such as a mouse, printer, monitor, game controller, video card, or any other peripheral equipment.

**device driver** – a small program that enables a device to communicate with the operating system. A device driver "talks" to the hardware device and "talks" to the operating system, functioning as a type of communication liaison between hardware and software.

**directory** – the organization of folders and subfolders on any given storage media.

**drive-by downloads** – files found on poisoned Web sites which download Trojan horses, spyware, viruses or other malware without the user's knowledge or consent.

**encryption** – the process of converting data into an unreadable form of text.

**endpoint** – any intelligent computing device (such as a server, desktop or laptop computer, tablet, or handheld computer that has a CPU and is capable of running application software) connected to others in a network.

**farm** – a bank of servers used to provide services to a network.

**firewall** – a security barrier that prevents unauthorized access to or from private networks.

**Get-Help** – PowerShell cmdlet that displays help about PowerShell cmdlets and concepts.

**Get-Process** – PowerShell cmdlet that retrieves a list of all processes running on the machine.

**Get-Service** – PowerShell cmdlet that retrieves a list of all services running on the machine.

**hacker** – any person who attempts to gain unauthorized access to a computer system.

**hash** – a number generated by an algorithm from a string of text. The hash is as unique to the text string as fingerprints are to an individual. Also called a message digest.

**hash encryption** – an encryption method in which hashes are used to verify the integrity of transmitted messages. Also called one-way encryption.

**hosted (Type 2)** – hypervisor software that runs on top of an operating system.

**hypervisor** – the software that runs one or more virtual machines.

**image** – a template or master copy of a virtual machine used in MED-V implementations.

**key** – a piece of information that determines the output of an encrypting algorithm. Encrypted text cannot be read without the correct decryption key to decrypt, or decipher, the encrypted data back into plaintext.

**load balancer** – a tool used to even out the workload across host servers and ensure that response time is minimized for all clients.

**malware (malicious software)** – refers to programs or files whose specific intent is to harm computer systems. Malware is an electronic form of vandalism that can have global implications.

**MED-V** – virtualization software that is designed for enterprises; it allows you to use a centralized system management tool to create, configure, and deploy virtual Windows machines to end user computers.

**network** – a group of two or more computers connected in such a way that they can communicate, share resources and exchange data with one another.

**operating system** – a software program that controls all hardware and application software on the computer.

**operating system edition** – a specific distribution of an operating system that determines which features are available.

**operating system version** – a reference to the specific code base that was used to develop the operating system. Examples include Windows XP, Windows Vista, and Windows 7.

**patch** – a file of programming code that is inserted into an existing executable program to fix a known problem, or bug. Patches are designed to provide an immediate but temporary solution to a particular programming problem.

**peer-to-peer network** — a network in which all the participating computers are more or less equal, and there is no central server or centralized management of network resources.

**permission bits** – file bits that the owner of a file can set to allow or disallow access to other users.

NTFS allows you to set permission bits.

**permissions** – rules associated with objects on a computer, such as files, folders and settings. Permissions determine whether you can access an object and what you can do with it.

**poisoned Web sites** – Web sites that contain malicious content designed to harm computers. Simply visiting a poisoned Web site can infect or destroy the data stored on a system.

**restore point** – a component of Windows ME, XP, Vista and Windows 7 that allows you to roll back system files, registry keys and installed programs to a previous state. You can think of a restore point as a saved "snapshot" of a computer's data and settings at a specific point in time.

**root directory** – the highest level of any directory.

**sandbox** – a security mechanism that keeps running programs separated from one another, and provides a tightly controlled set of resources for guest programs to run in.

**server** – a computer in the network that manages network resources and/or provides information and services to clients on the network

**sequencing** – in APP-V, sequenced applications are streamed to client computers from a centralized server, but appear to be installed on the local machine.

**service** – an application program that runs in the background.

**service pack** – a collection of updates typically released after enough updates have accumulated to warrant the release. Service packs typically contain all previous updates, which include security patches, bug fixes, new features, utilities and applications.

**spyware** – a software application that is secretly placed on a user's system and gathers personal or private information without the user's consent or knowledge.

**streaming** – the process of transferring data or applications from a server to a client in a continuous data stream. App-V applications are

**symmetric-key encryption** – an encryption method in which one key is used to encrypt and decrypt messages. Also known as single-key encryption.

**system drive** – the hard drive on which the operating system is installed.

**time out** – an event that occurs at the end of a predetermined period of time to prevent a system from waiting indefinitely for something to happen. A predetermined waiting period will be aborted after the timeout period has elapsed.

**Trojan horse** – a program designed to allow a hacker remote access to a target computer system. Unlike worms and viruses, Trojan horses do not replicate themselves or copy themselves to other files and disks.

**update** – any file or collection of software tools that resolves system liabilities and improves software performance. Updates are released periodically when deemed necessary by the vendor.

**upgrade** – a method of installing Windows wherein all existing user settings, files and installed applications are retained and you do not need to reinstall them.

**usage policy** – configurations specific to a MED-V image; used to identify which users are permitted access to the image, and stored in Active Directory.

**virtual** – in computing, refers to the way a particular component or environment appears to a user.

**virtual machine (VM)** – a simulated collection of computer hardware that exists and behaves like a real (physical) computer, but is in fact a software implementation of a computing environment. You create a VM using virtualization software.

**virus** – a malicious program designed to damage computer systems. Viruses are loaded onto your computer without your knowledge and run without your consent

**workspaces** – Windows virtual machines created with MED-V software.

**worm** – a self-replicating program that consumes system and network resources. A worm automatically spreads from one computer to another without requiring human action.

**x64** – a reference to the 64-bit class of processors.

**x86** – a reference to the 32-bit class of processors

**XP Mode** – virtualization software which enables you to create and run a Windows XP virtual machine on your Windows 7 Desktop.


# Index




## T



## U



## V



## W



## X



## Z