LESSON 4.1

10753 Windows Operating System Fundamentals

# Understand File Systems

LESSON 4.1

98-349 Windows Operating System Fundamentals

# Lesson Overview

Understanding file systems.

In this lesson, you will:

- Explore various file system types.
- Identify file system types.
- Convert existing file systems.

# File System Type: FAT

- FAT
  - The file allocation table (FAT) is located at the beginning of a logical volume. FAT was designed for small disks and simple folder structures.
- Two copies of the FAT are stored on the volume.
  - If one copy of the FAT becomes corrupted, the other FAT is used.

# FAT File System

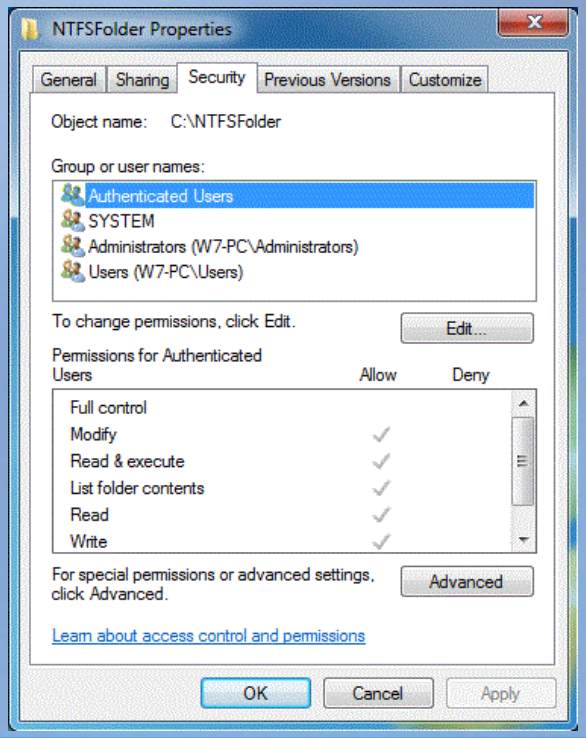
- FAT16—MS-DOS through Microsoft Windows 2000:
  - Maximum drive size was limited to 4 GB.
  - Maximum volume size was limited to 2 GB.
  - There was no built-in file system security or compression.
- FAT32—Windows 95OSR2 to present:
  - Maximum volume size was limited to 32 GB.
  - The file size limit was 4 GB.
  - There was no built-in file system security or compression.

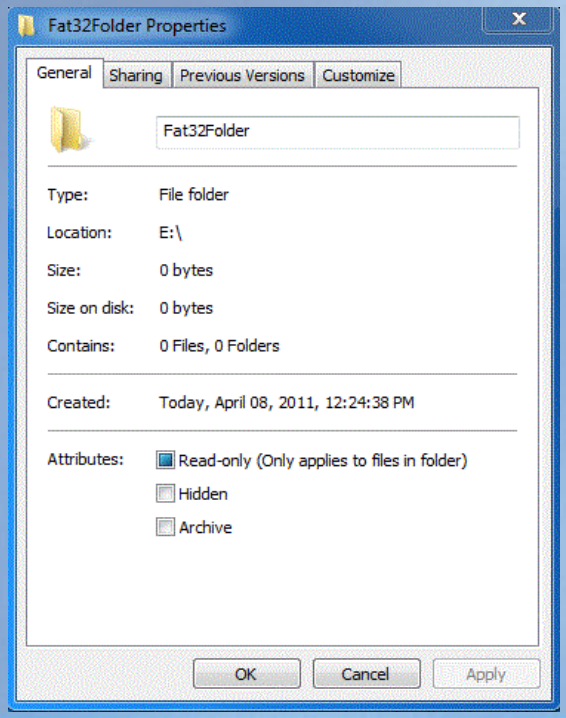
# File System Type: NT File System (NTFS)

- NTFS is the preferred Windows file system for Microsoft Windows NT.
- Has the capability to recover from some disk-related errors automatically. (FAT32 does not have this ability.)
- Maximum file size is 16 TB.
- Supports larger hard drives.
  - The recommended size is 2 TB, but much larger sizes are possible (up to 256 TB).
- Provides better security through the use of NTFS permissions and encryption to restrict access to specific files and approved users.

# NTFS

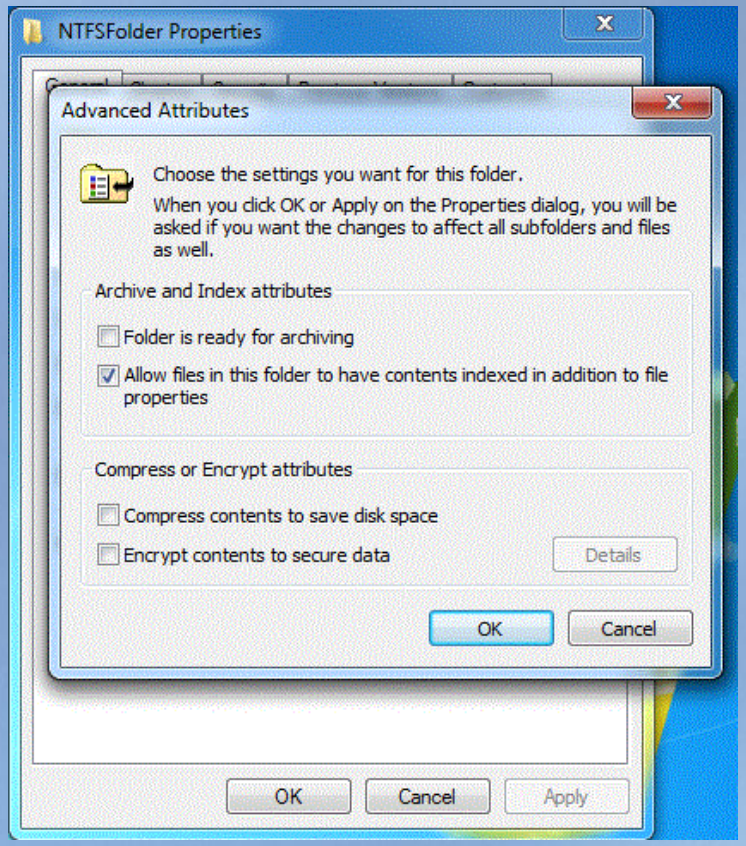
- The folder created on an NTFS volume (left) enables the user to secure the resource as displayed on the Security tab. The Fat32Folder (right), created on a FAT32 volume, does not.



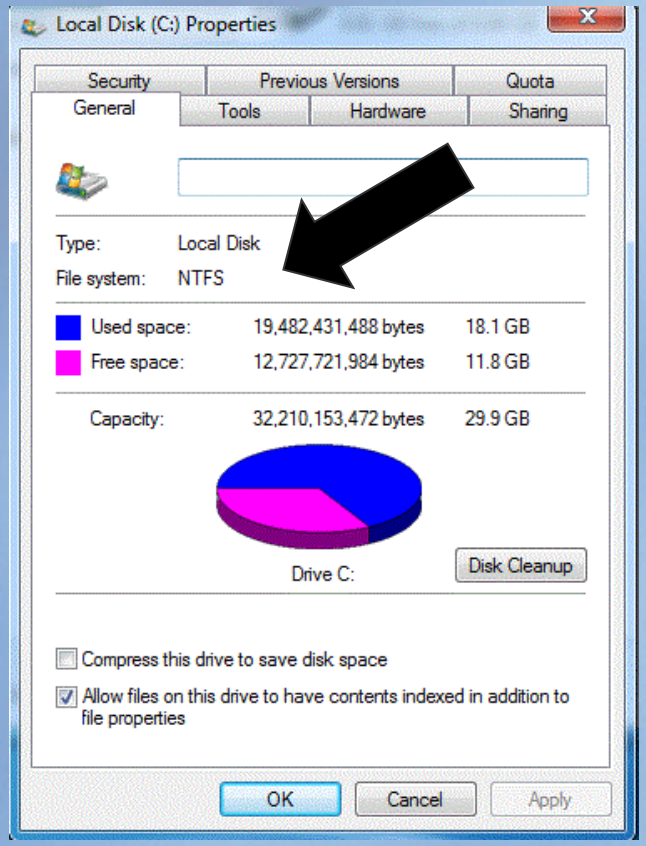
# NTFS (continued)

- Formatted volumes allow for compression and encryption.



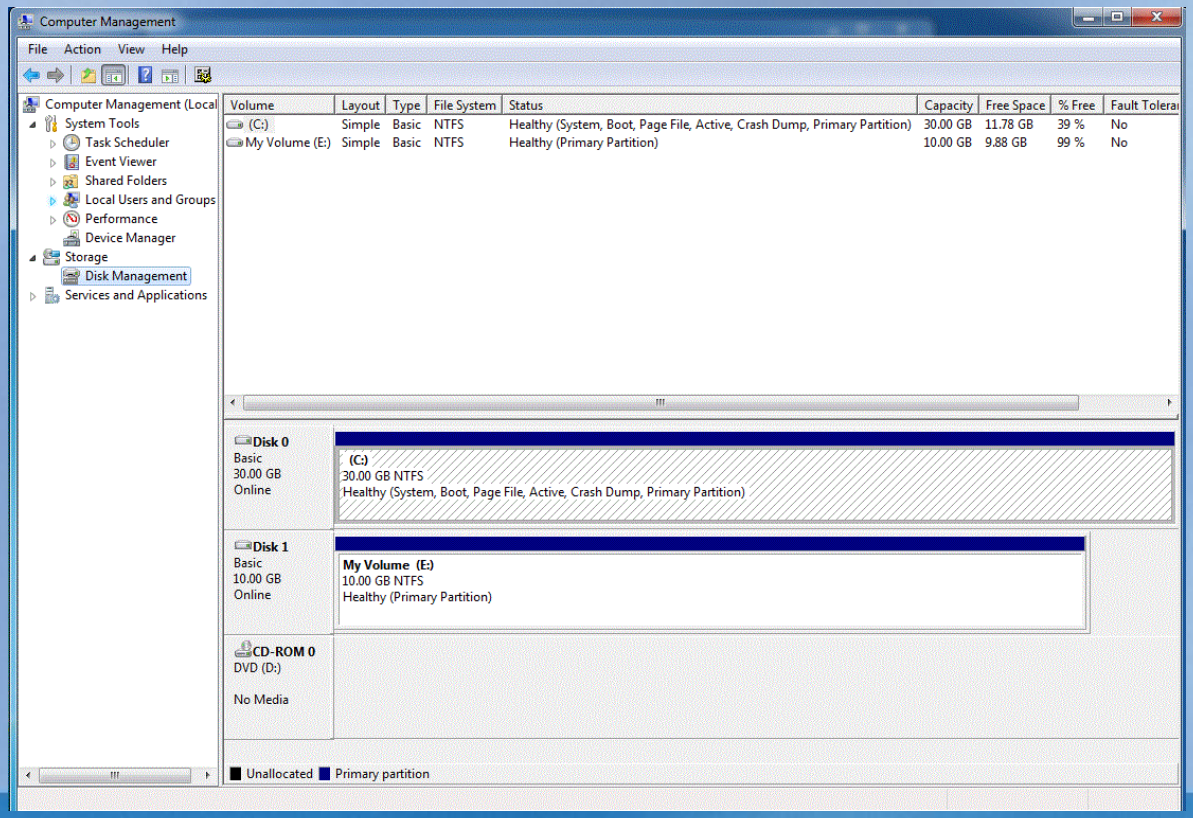
# Identifying File System Type

- Identify the file system type using the graphical user interface (GUI) or the command-line interface (CLI).
- One method using the GUI:
  - Click Start, then click Computer.
  - Under Hard Disk Drives, right-click a drive and click Properties.
  - The file system that the drive uses is listed on the General tab under File System as shown here.



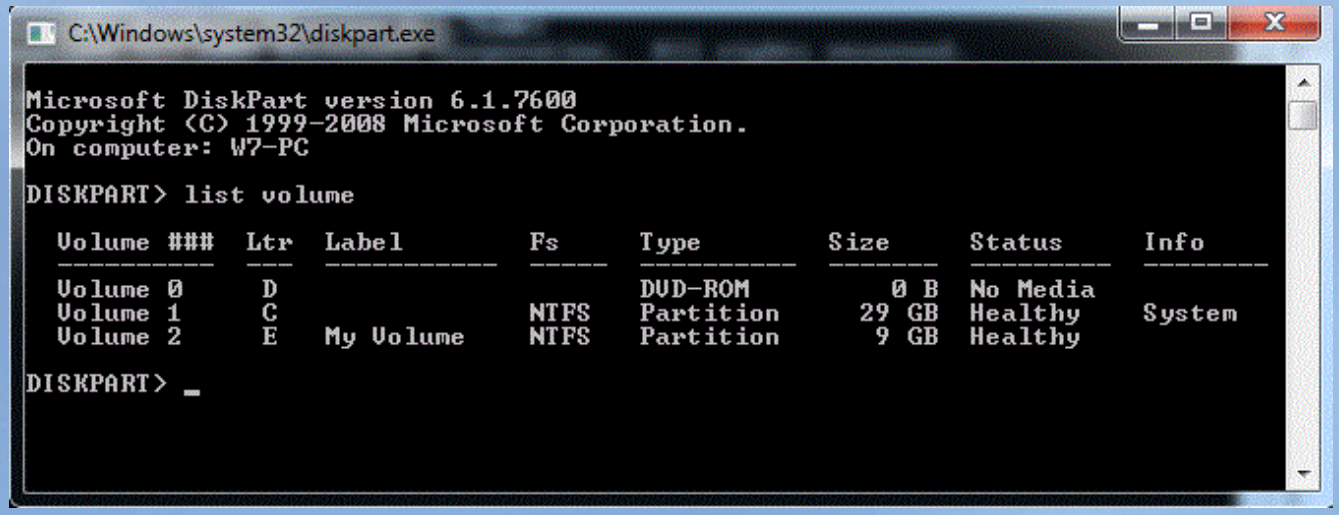
# Identifying File System Type (continued)

- Another method within the GUI is to open the Disk Management console by clicking Start, typing **disk management**, and pressing ENTER.



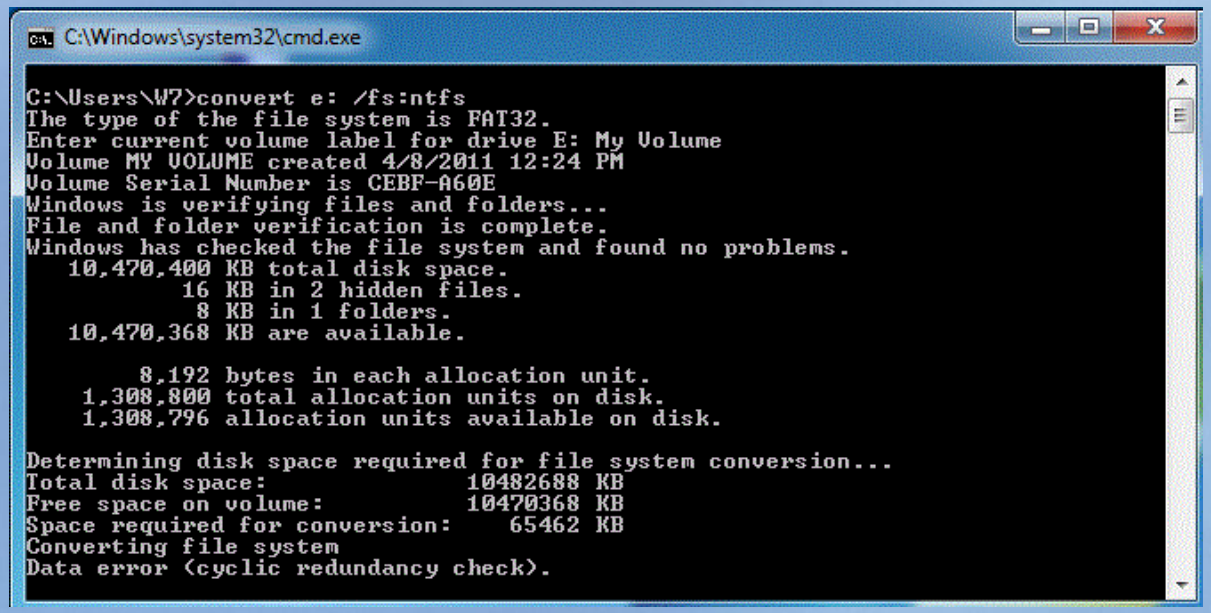
# Identifying File System Type (continued)

- And another method is using the Command Line Interface:
  - Click Start. Type **command prompt** in the Search box and press ENTER.
  - Acknowledge UAC.
  - At the CLI, type **diskpart** and press ENTER.
  - Type **list volume** and press ENTER. Compare with the following image:



# Converting Existing File Systems

- Convert an existing a FAT32 to NTFS using the CLI.
- Click Start. Type **command prompt** in the Search box and press ENTER.
- To convert the E volume to NTFS, type **convert E: /fs:ntfs** and press ENTER.



# Converting Existing File Systems (continued)

- Most external drives (USB, external hard drive) are formatted in FAT32 when purchased. This is important to note due to security reasons.
- When you convert from NTFS to FAT32, keep the following in mind:
  - All data on volume will be lost. Back up your data prior to formatting.
  - Format the volume using NTFS.

LESSON 4.1

98-349 Windows Operating System Fundamentals

# Complete Student Activity 4.1

LESSON 4.2

98-349 Windows Operating System Fundamentals

# Understand File and Print Sharing

LESSON 4.2

98-349 Windows Operating System Fundamentals

# Lesson Overview

Understand file and print sharing.

In this lesson, you will explore:

- NTFS permissions
- File sharing
- Printer sharing
- Connecting to shared resources

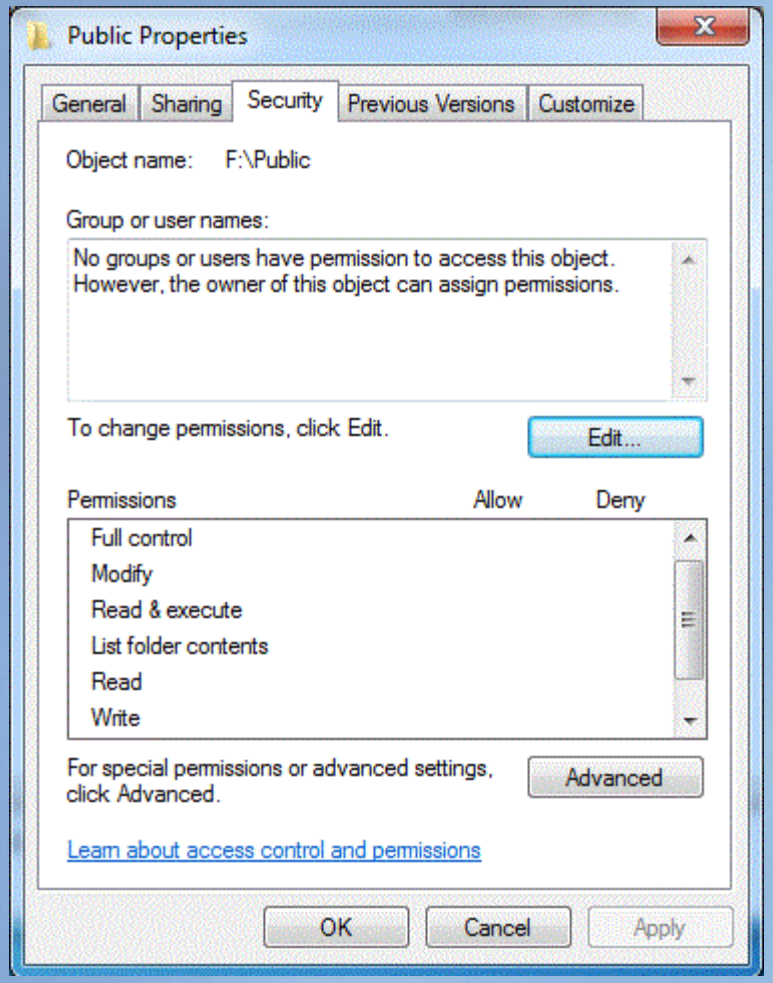
# NTFS Permissions

When securing a computer and its resources, you will perform the following tasks:

- Evaluate the rights that users will need.
- Grant users or groups specific user rights.
- Secure an object, such as a file or folder, by assigning permissions to allow users or groups to perform specific actions on that object.

# NTFS Permissions (continued)

- Granting Full Control NTFS permission on a folder to a user enables that user to take ownership of the folder.
- Be cautious in granting Full Control. Always grant the minimum rights for a user to perform their tasks
- NTFS permissions affect access both locally and remotely.



# NTFS Permissions (continued)

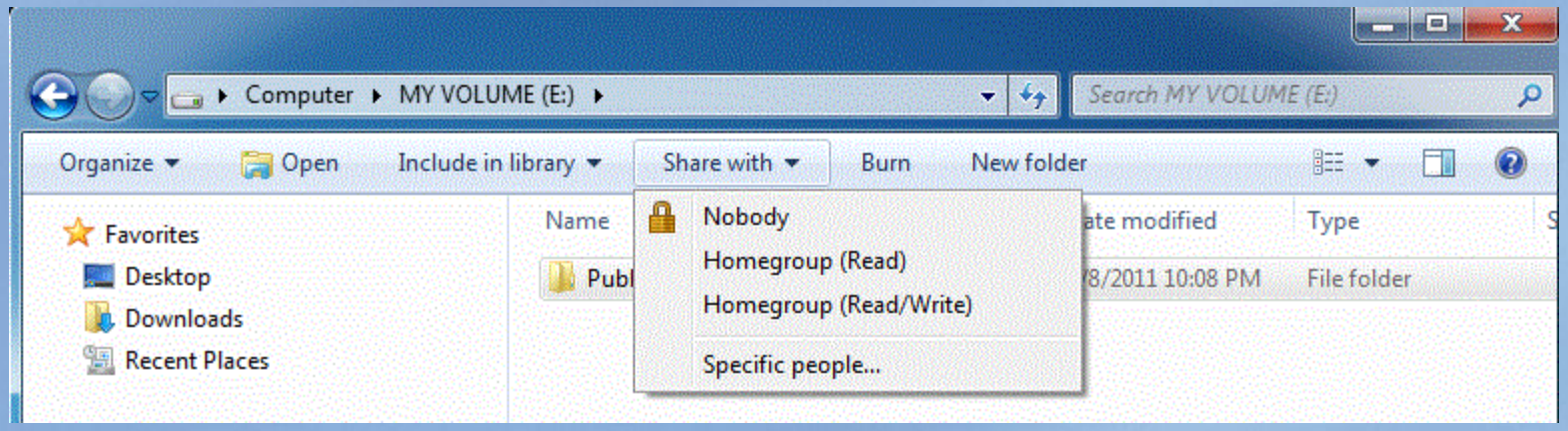
- **Full Control:** Users can see the contents of a file or folder, change files and folders, create files and folders, and run programs in a folder. Users can modify the access control and take ownership of a resource.
- **Modify**: Users can change existing files and folders. create new files and folders, and delete files and folders.
- **List Folder Contents**: Users can view and list files and subfolders as well as execute files; this permission is inherited only by folders.
- **Read & Execute:** Users can see the contents of existing files and folders and can run programs in a folder.
- **Write:** Users can create new files and folders and make changes to existing files and folders.
- **Read**: Users can see the contents of a folder and open files and folders.

# File Sharing

- A shared resource is made available to network users. These resources include folders, files, and printers.
- The term *shared resource* also can refer to a resource on a server that is available to network users. When you share a resource, you use share permissions.
- When accessing the resource across the network, both NTFS and share permissions apply; however, the most restrictive of the permissions will be the effective permissions.

# File Sharing—Windows 7 Homegroups

- A homegroup is a group of computers on a home network that can share files and printers.
- It is a convenient way to share music, pictures, and documents automatically.
- You can also select the Share With Menu option to share folders and files that aren't shared automatically.

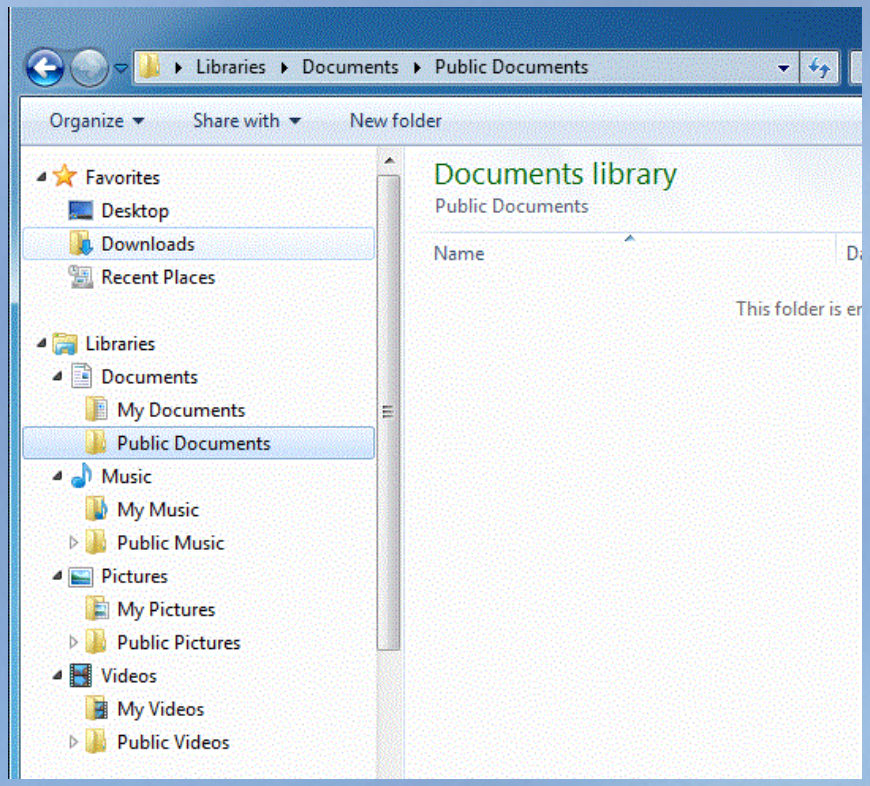


# File Sharing—Windows 7 Homegroups (continued)

- The most common menu options are:
  - **Nobody:** makes an item private so only you have access.
  - **Homegroup (Read):** the homegroup has read-only permission.
  - **Homegroup (Read/Write):** the homegroup has read/write permissions.
  - **Specific People:** uses the File Sharing Wizard so you can choose who to share with.
- **Read**: users can open, but cannot change or delete a file.
- **Read/Write**: users can open, modify, or delete a file.

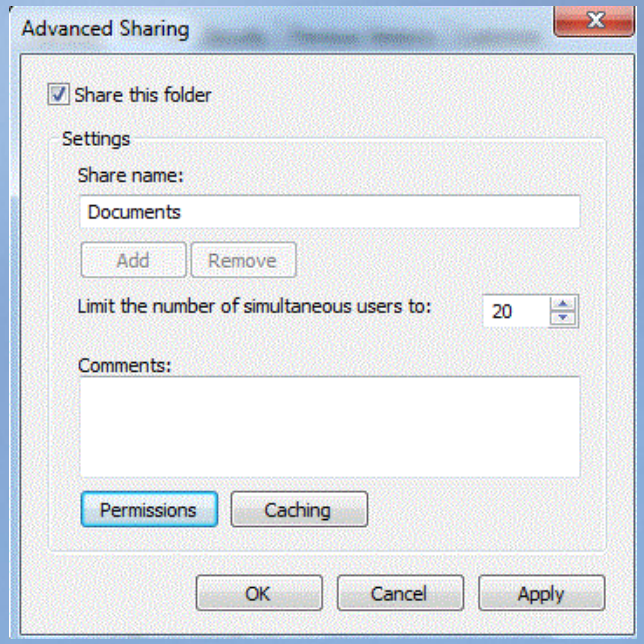
# Public Folder Sharing

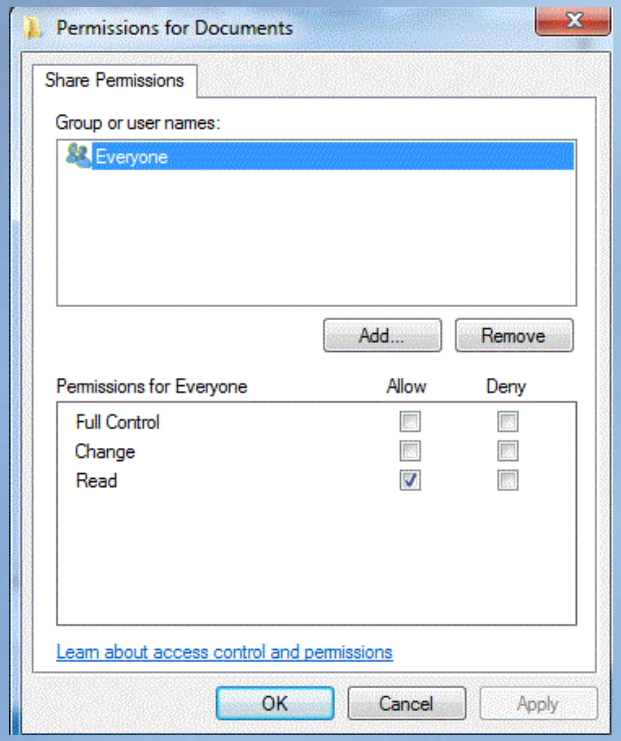
- Turned off by default.
- Files can be shared by dropping files in the Public folder (Windows 7).



# Advanced Sharing

- Offers more control over sharing resources.
- Right-click the folder, select Properties, then click the Sharing tab. Click the Advanced Sharing button.



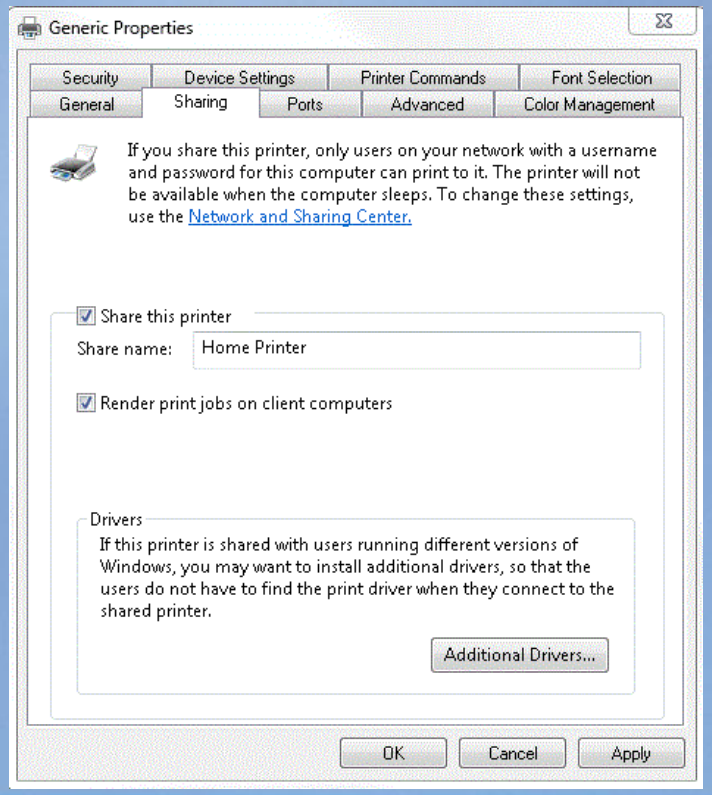



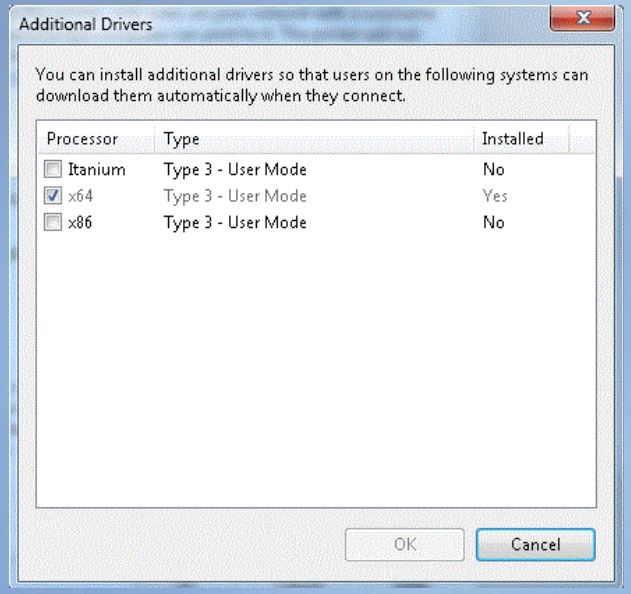
LESSON 4.2

98-349 Windows Operating System Fundamentals

# Printer Sharing

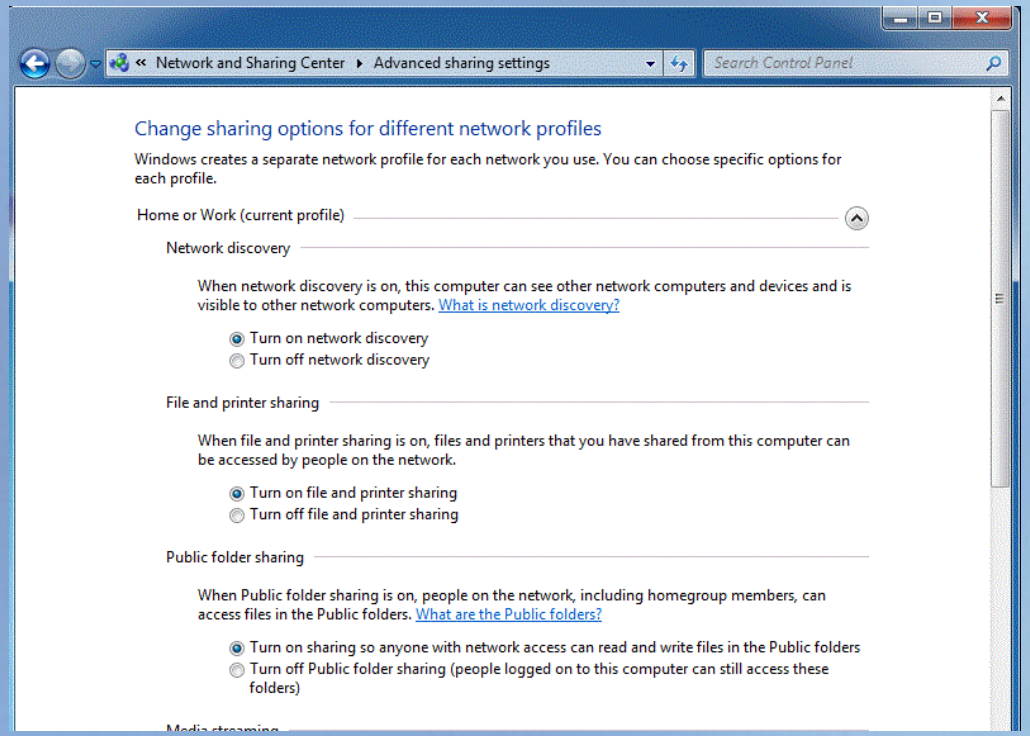
- Allows multiple computers on a network to use a single printer.



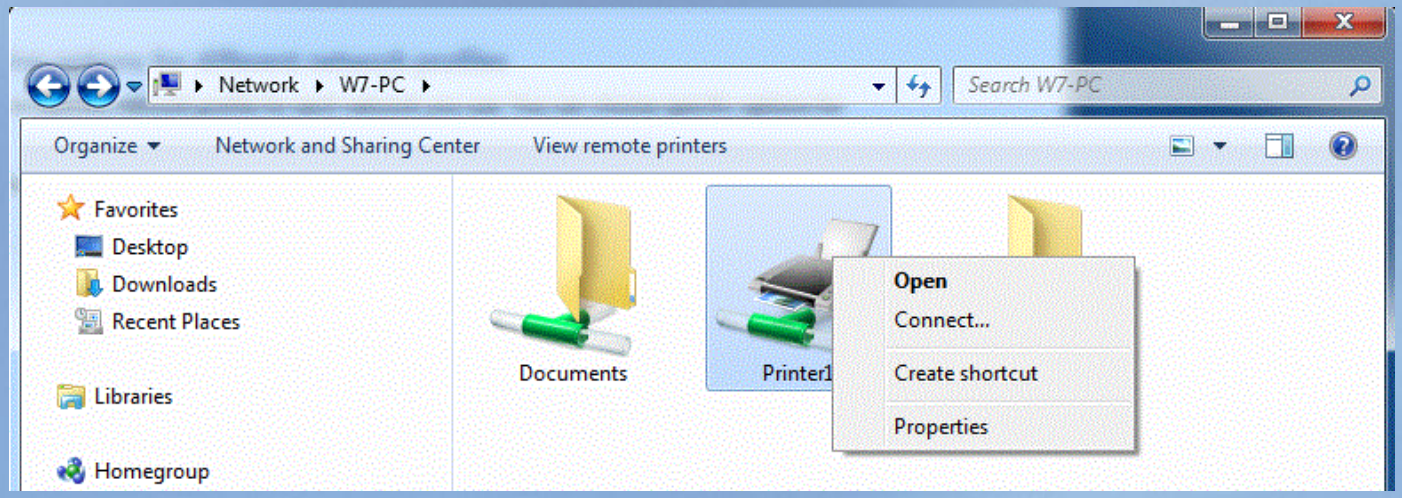
# Printer Sharing (continued)

- Enable printer sharing through a firewall as follows:
  - Click Start.
  - Open Control Panel.
  - Click Network And Internet.
  - Click Network And Sharing Center.
  - Click Change Advanced Sharing Settings.



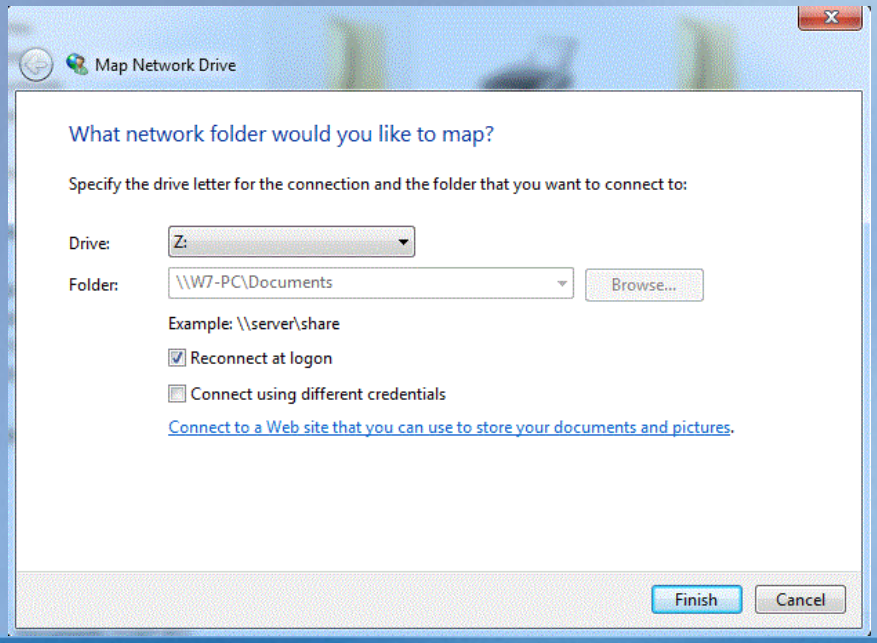
# Connecting to Shared Resources

- Connect shared resources by clicking the Network icon in Windows Explorer and selecting the computer that is sharing the resources.
- For printers, right-click the device and select Connect. This will install the appropriate driver and make the shared printer available on your computer.



# Connecting to Shared Resources (continued)

- Right-click a shared folder and select Map Network Drive to make the folder available through Windows Explorer using a drive letter identifier.
- The mapped network drive will be displayed in Windows Explorer under Network Locations.



# Complete Student Activity 4.2

LESSON 4.3

98-349 Windows Operating System Fundamentals

# Understand Encryption

LESSON 4.3

98-349 Windows Operating System Fundamentals

# Lesson Overview

Understanding encryption.

In this lesson, you will explore:

- Encryption
- BitLocker
- File and folder compression

# Encryption

- Encryption is the process of coding plain text to create cipher text.
- Two types of encryption:
  - Symmetric key encryption—uses the same key for encrypting and decrypting information.
  - Public (asymmetric) key encryption—uses different keys for encrypting and decrypting information.
- Public key encryption is used to perform the following functions:
  - Encrypting symmetric secret keys to protect the keys during exchange over the network or while being used, stored, or cached by operating systems.
  - Creating digital signatures to provide authentication and nonrepudiation for online entities.
  - Creating digital signatures to provide data integrity for electronic files and documents.

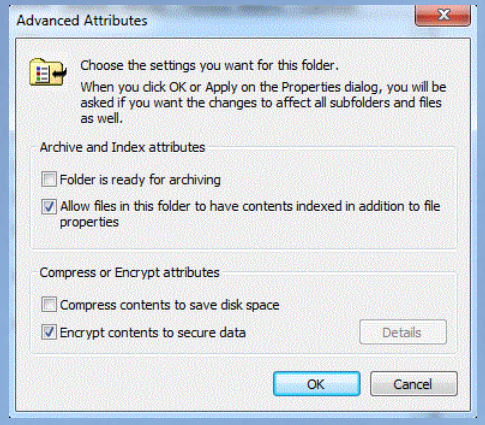
# Encryption (continued)

- EFS enables transparent encryption and decryption of files by using advanced, standard cryptographic algorithms.
- EFS isn't designed to protect data while it's transferred from one system to another.
- EFS doesn’t occur at the application level, but at the file-system level. Encryption and decryption is transparent to the user.
- EFS uses a symmetric key, which itself is encrypted with a the public key of a public key encryption pair. The private key must be available for the file to be decrypted. The key pair is bound to the user identity by the user ID and password.
- EFS keys can be archived.
- EFS keys are protected by the user’s password.

# Encryption (continued)

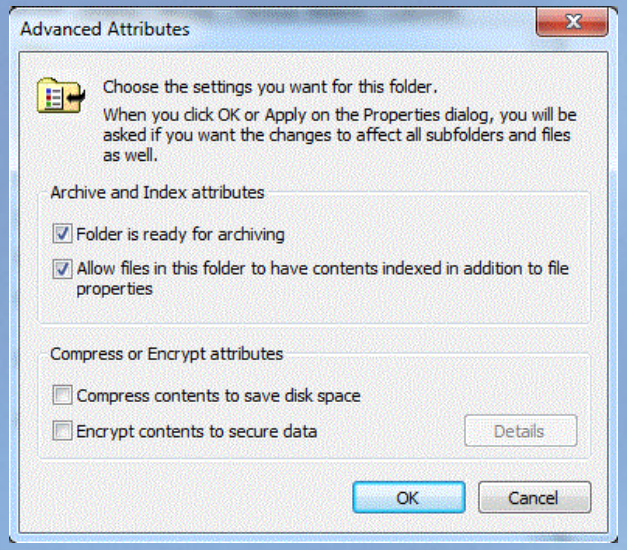
- **Encrypt a file or folder**
  1. Right-click the folder or file to encrypt and select Properties.
  2. Click the General tab and then click Advanced
  3. Select the Encrypt Contents To Secure Data check box and click OK.

Note: It is important to back up your encryption certificate. If you lose or damage your certificate or key, your data will be lost.



# Encryption (continued)

- **Decrypt a file or folder**
  1. Right-click the folder or file to decrypt and select Properties.
  2. Click the General tab and then click Advanced
  3. Clear the Encrypt Contents To Secure Data check box and click OK.



# BitLocker

- BitLocker Drive Encryption - data protection feature available in Windows 7 Ultimate and Enterprise editions.
- BitLocker To Go - data protection feature to lock portable storage devices.
- BitLocker is installed automatically as part of the operating system.
- BitLocker is not enabled until it is turned on using the BitLocker setup.
- A Trusted Platform Module (TPM) can be used with BitLocker to provide the most protection. The TPM is a hardware component installed with most newer computers.
  - BitLocker can still be used on computers that do not have a TPM. It requires a USB startup key to start the computer.
- BitLocker offers the option to lock the normal startup process until a user supplies a personal identification number or inserts a removable device.

# BitLocker (continued)

- **Turn on Bitlocker**

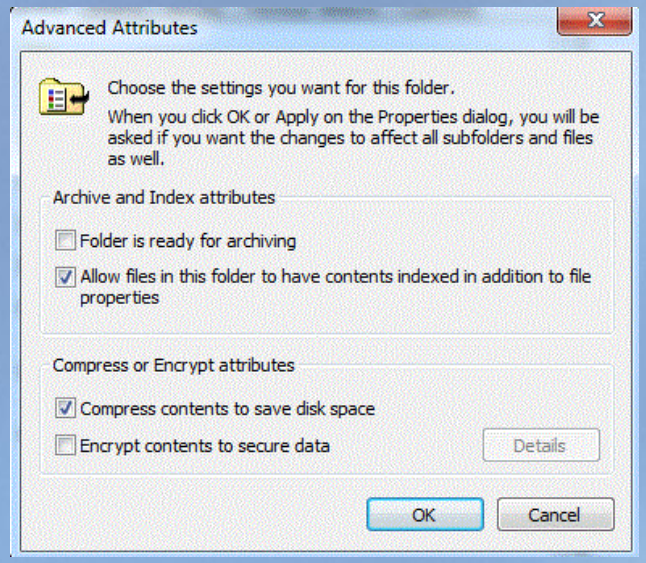
1. Click Start, Control Panel, System and Security, and then BitLocker Drive Encryption.
2. Choose a drive to secure and click Turn On BitLocker. This will start the BitLocker setup wizard.
3. Choose a method to unlock the drive, either by password or smart card.
4. Choose either to save the recovery key to a file or print it.
5. Click Start Encrypting.

# File and Folder Compression

- File compression on an operating system can be used to conserve disk space; however, it also can degrade your system's performance.
  - For instance, when you move a compressed file to a different folder, the system decompresses the file, moves the file to the new location, and then compresses it again. This happens both locally and across the network.
- Windows also supports compressing individual files as compressed (zipped) folders.
  - All files and folders are compressed into a single file with the .zip extension.

# File and Folder Compression (continued)

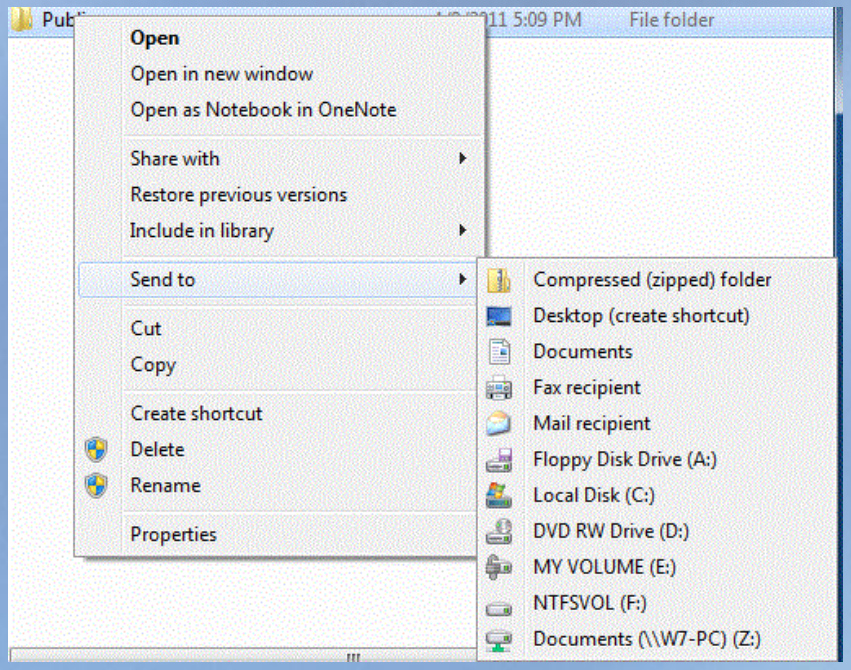
- **Compress a file or folder**
  1. Right-click the folder or file to compress and select Properties.
  2. Click the General tab and then click Advanced.
  3. Select Compress Contents To Save Disk Space check box and click OK.



# File and Folder Compression (continued)

- **Compressing a file or folder to a zipped folder**

1. Right-click the folder or file to compress, select Send To, and choose Compressed (Zipped) Folder.



LESSON 4.3

98-349 Windows Operating System Fundamentals

# Complete Student Activity 4.3

LESSON 4.4

98-349 Windows Operating System Fundamentals

# Understand Libraries

# Lesson Overview

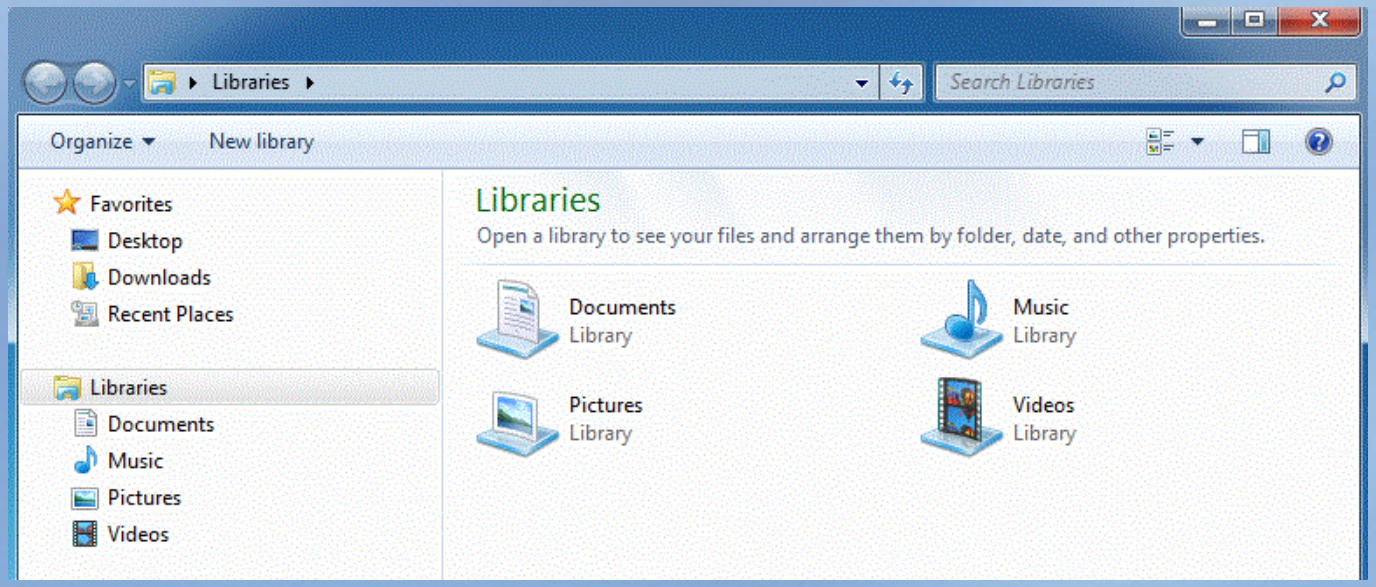
Understand libraries.

In this lesson, you will explore:

- Configuring libraries
- Configuring offline files

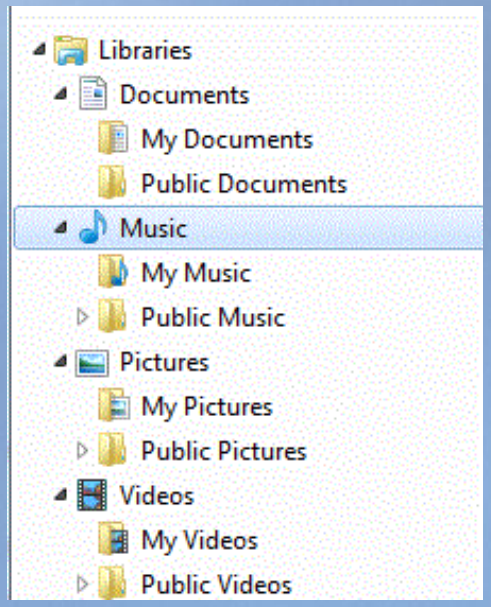
# Libraries

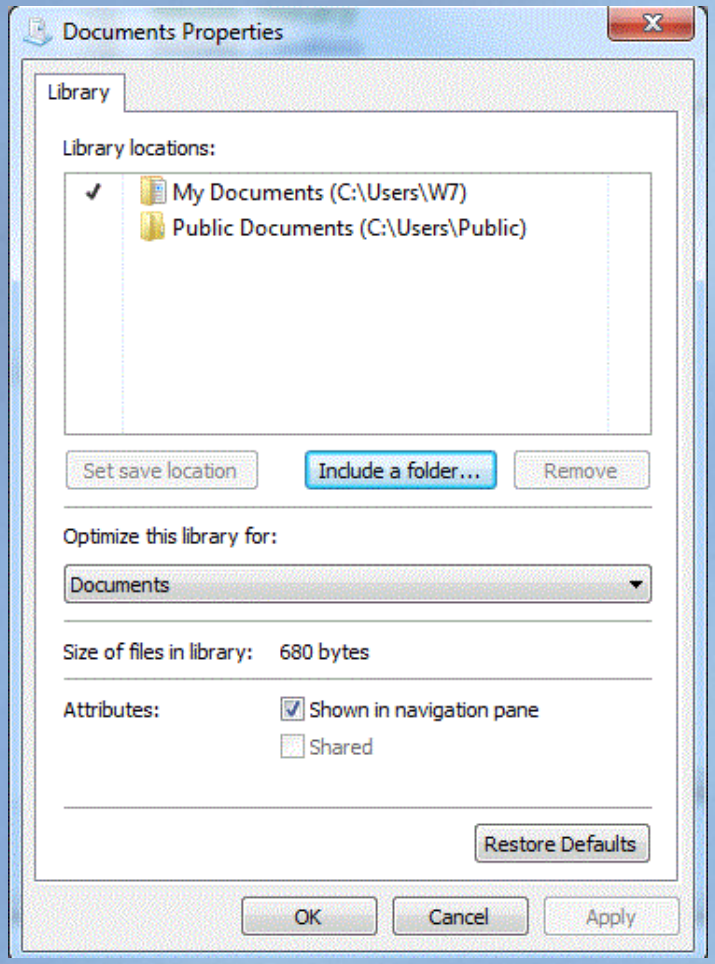
- Libraries manage documents, music, pictures, and other files.
- Browse files in the same way that you would in a folder, or view files arranged by properties such as date, type, and author.



# Libraries (continued)

- Default libraries include:
  - Documents
  - Music
  - Pictures
  - Videos



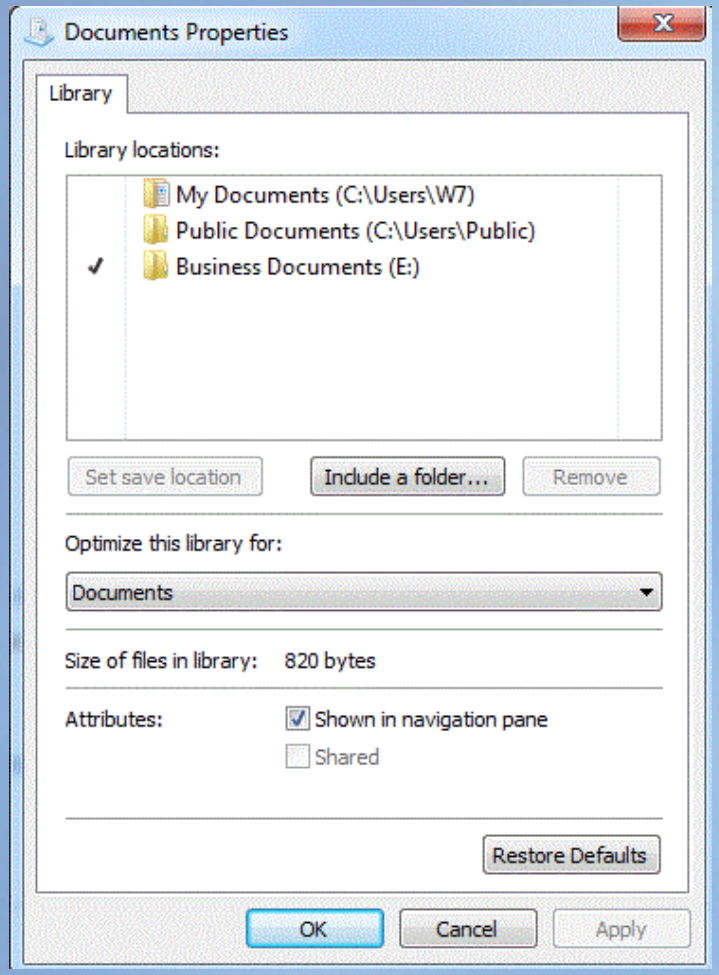



# Libraries (continued)

- A library gathers files from different locations and displays them as a single collection without moving them from where they're stored.
- Tasks:
  - Create a new library.
  - Arrange items by folder, date, and other attributes.
  - Include or remove folders.
  - Change the default save location.

# Adding a Location to a Library

- Open Windows Explorer and expand the Library folder.
- Right-click the Documents library and select Properties.
- Click Include A Folder and browse to the folder to be added to the library.
- The default save location for file types can be changed by highlighting the library location and clicking Set Save Location.



# Offline Files

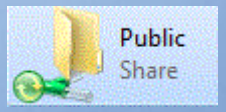
- Benefits:
  - Files are unaffected by network outages.
  - Files can be worked with while away from the network.
  - Files are synched easily with network files.
  - User efficiency is increased when working over a slow network.

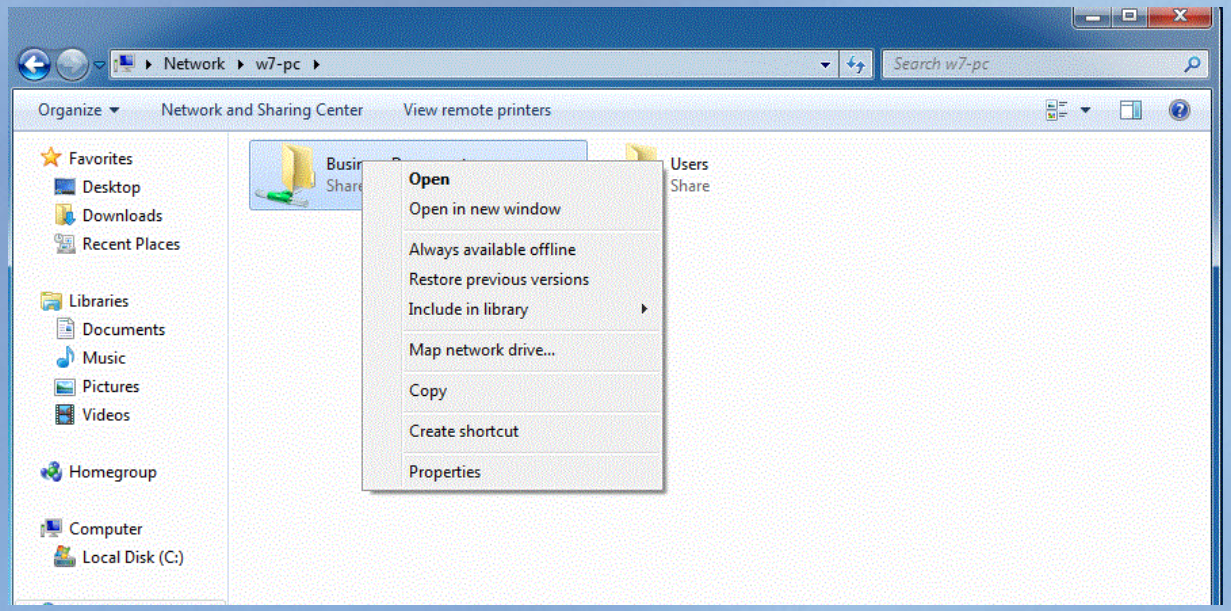
# Offline Files (continued)

- Enhancements in Windows 7:
  - Transparent caching on clients for shared folders reduces the time required to access files across a slow network after the first time. This is combined with protocol enhancements that eliminate multiple, redundant network operations when opening or saving files to provide an improved application experience across slow networks.
  - Background synchronization capabilities for offline files reduce administrative overhead and enhance the user experience.

# Configuring Offline Files

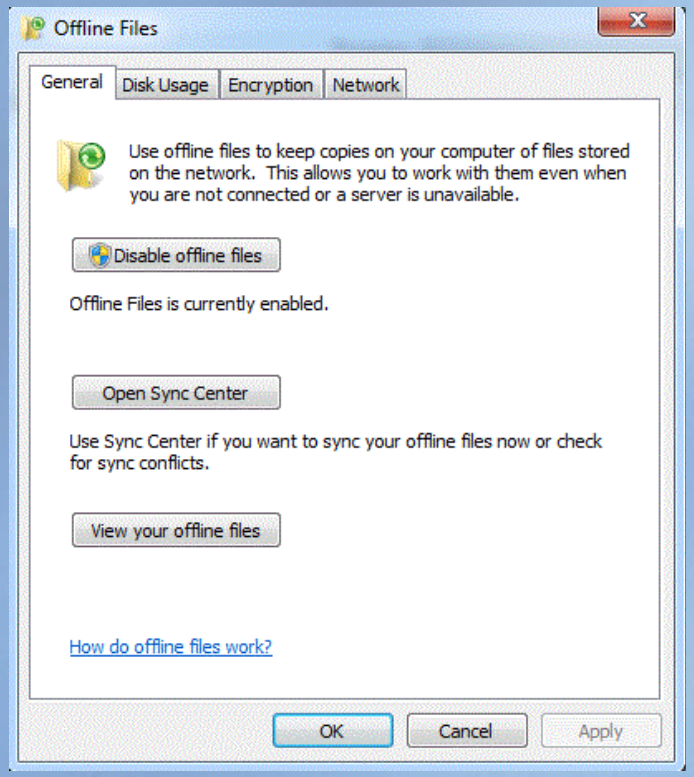
- Make a folder available offline as follows:
  - Connect to the resource over the network.
  - Right-click the folder or share and select Always Available Offline. The folder will be represented with a synchronized icon.



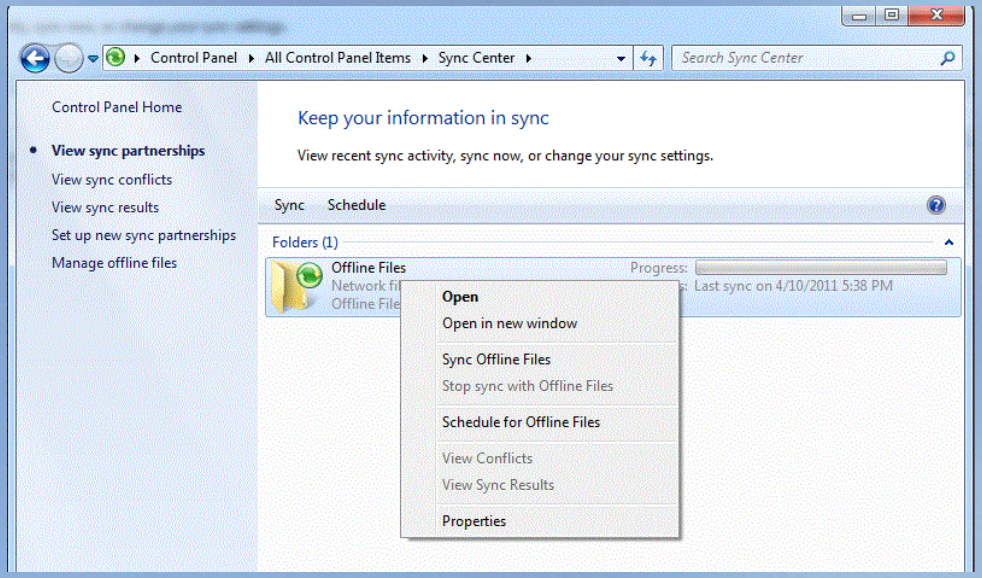
# Configuring Offline Files (continued)

- Manage offline files as follows:
  - Click Start
  - Type offline files in the Search Programs And Files field
  - Press ENTER



# Configuring Offline Files (continued)

- If you wish to ensure that your folders is synchronized before going offline, you can force synchronization of a folder marked for offline access.
  - Within Sync Center, right-click the folder and select Sync Offline Files.



LESSON 4.4

98-349 Windows Operating System Fundamentals

# Complete Student Activity 4.4