Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**5**

**Managing Disks and File Systems**

* [Chapter Introduction](javascript://)
* **5-1**[Disk Technology](javascript://)
  + **5-1a**[Internal Disk](javascript://)
  + **5-1b**[External Disk](javascript://)
  + **5-1c**[Virtual Hard Disk (VHD)](javascript://)
  + **5-1d**[Multiple Disks as One Logical Disk](javascript://)
* **5-2**[Disk Partition Styles](javascript://)
* **5-3**[Disk Types](javascript://)
  + **5-3a**[Basic Disks](javascript://)
  + **5-3b**[Dynamic Disks](javascript://)
  + **5-3c**[Storage Spaces](javascript://)
* **5-4**[Disk Management Tools](javascript://)
  + **5-4a**[Disk Management Console](javascript://)
  + **5-4b**[DiskPart](javascript://)
  + **5-4c**[Storage Cmdlets in Windows PowerShell](javascript://)
* **5-5**[Managing Physical Disks](javascript://)
  + **5-5a**[Adding a New Drive](javascript://)
  + **5-5b**[Moving Drives](javascript://)
* **5-6**[Virtual Disk Management Tasks](javascript://)
  + **5-6a**[Creating VHDs](javascript://)
  + **5-6b**[Attaching and Detaching VHDs](javascript://)
* **5-7**[Managing Storage Spaces](javascript://)
  + **5-7a**[Creating an Initial Storage Pool and Storage Space](javascript://)
  + **5-7b**[Maintaining Storage Pools and Storage Spaces](javascript://)
  + **5-7c**[Configuring Storage Spaces Fault Tolerance](javascript://)
* **5-8**[File Systems](javascript://)
  + **5-8a**[File Allocation Table (FAT)](javascript://)
  + **5-8b**[New Technology File System (NTFS)](javascript://)
  + **5-8c**[Resilient File System (ReFS)](javascript://)
  + **5-8d**[Universal Disk Format (UDF)](javascript://)
* **5-9**[File System Tasks](javascript://)
  + **5-9a**[Changing Drive Letters](javascript://)
  + **5-9b**[Converting File Systems](javascript://)
* **5-10**[File and Folder Attributes](javascript://)
  + **5-10a**[Managing Attributes](javascript://)
  + **5-10b**[Copying and Moving Compressed Files](javascript://)
* **5-11**[File and Folder Permissions](javascript://)
  + **5-11a**[Default Folder Permissions](javascript://)
  + **5-11b**[Basic NTFS Permissions](javascript://)
  + **5-11c**[Advanced NTFS Permissions](javascript://)
  + **5-11d**[Permission Scope](javascript://)
  + **5-11e**[Permission Inheritance](javascript://)
  + **5-11f**[Effective Permissions](javascript://)
  + **5-11g**[Ownership](javascript://)
  + **5-11h**[Permission Changes When Content Is Copied or Moved](javascript://)
  + **5-11i**[Permission Strategy Considerations](javascript://)
* **5-12**[File Sharing](javascript://)
  + **5-12a**[Sharing Individual Files](javascript://)
  + **5-12b**[Sharing the Public Folder](javascript://)
  + **5-12c**[Creating and Managing Shared Folders](javascript://)
  + **5-12d**[Monitoring Shared Folders](javascript://)
* **5-13**[Chapter Review](javascript://)
  + **5-13a**[Summary](javascript://)
  + **5-13b**[Key Terms](javascript://)
  + **5-13c**[Review Questions](javascript://)
  + **5-13d**[Case Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After reading this module and completing the exercises, you will be able to:

* **1**Describe disk technologies and partition styles
* **2**Distinguish between basic, dynamic, and Storage Spaces disk types
* **3**Use disk management tools
* **4**Describe and manage physical disks
* **5**Create and manage virtual hard disks (VHDs)
* **6**Describe Storage Spaces components such as storage pools, storage space volumes, and resilience
* **7**Describe Windows 10 supported file systems and their features, limits, and tasks
* **8**List file and folder attributes used in Windows 10 file systems
* **9**Understand Windows 10 file and folder permissions
* **10**Describe Windows 10 file sharing methods and monitoring

This module looks at how storage is managed by Windows. Windows 10 combines old and new disk management technology, such as basic MBR disks, that have been around for decades and new software-controlled Storage Spaces technology with resiliency options. The module looks at how space on local disks is divided into units of storage called partitions or volumes. These volumes must be formatted with a file system to store and organize data, and Windows 10 has several file systems from which to choose. Different file systems include different management features. The management features can be basic, such as including management attributes to mark data as read-only, or hidden. Other management features can offer advanced security settings that control what specific identities can do with the data. In this module, you learn the factors involved in choosing various storage solutions.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-1**Disk Technology

Disk technology can be categorized by how it is connected to the computer and how it is presented to Windows 10. When you are reviewing disk technology available on a computer for use with Windows 10, consider these disk technologies:

* Internal disk
* External disk
* Virtual hard disk (VHD)
* Multiple disks as one logical disk

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1aInternal Disk

Devices that run Windows 10 are usually designed with consumer-grade technology and not server-grade components. Internal disks are commonly realized with electromechanical drives, solid-state drives, or custom embedded chip memory. Electromechanical drives are an older technology that rotate physical disks to read and write data, so they are slower, bulkier, and consume more power but provide storage at a lower cost. Solid-state drives (SSDs) with no moving parts are smaller and faster than electromechanical drives, but they are also more expensive and have a limited operational lifetime. Device manufacturers often embed chip memory into tablet devices running Windows 10 at the factory, some of which is used to emulate an internal disk drive. These common, nonremovable disk types are attached to the device’s internal interface(s) and provide a suitable location to store operating system files required to start the computer.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1bExternal Disk

External interfaces are used to connect removable, portable disk storage. External storage is useful for expanding a computer’s bulk file storage to contain application and user data files, but it is not typically suitable for operating system files that are essential and must always be present. Windows 10 is not normally installed on removable disk media.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1cVirtual Hard Disk (VHD)

A [**virtual hard disk (VHD)**](javascript://) is a file format that can be used by the operating system to emulate the function of a hard drive, with all the data and structural elements of a drive. Files can be stored in a VHD storage location just like any other disk technology once the VHD is attached and made available through the Windows 10 operating system. A VHD may contain thousands of individual files from the user’s perspective, but it still appears as only one physical file on the disk hosting that VHD file.

**Tip**

All versions of Windows 10 support VHD operations. For example, double-clicking a VHD file automatically opens the VHD file as a mounted drive on the local operating system.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-1dMultiple Disks as One Logical Disk

A logical disk appears to the Windows 10 operating system as one disk drive. Internal, external, and VHD disks are all examples of individual logical disks. Multiple drives can also be grouped together to appear as one logical disk to Windows 10. Two reasons for grouping multiple drives in this way include creating a logical disk that has more combined space than one disk alone could have and adding fault tolerance. The fault tolerance allows for a disk in a combined set to fail without losing access to the group’s logical disk and its data. Windows 10 includes Storage Spaces, which can also combine multiple disks as one logical disk using technology that is similar to RAID (Redundant Array of Independent Disks) but is enhanced beyond that legacy technology.

**Note 1**

For simplicity, the remainder of this module uses the term disk to refer to a logical disk.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 5-2Disk Partition Styles

When you configure a disk for use by Windows 10, you need to select a partition style. A partition style specifies how data can be organized on the disk. The [**GUID Partition Table (GPT)**](javascript://) is used with new computers that use UEFI firmware to start the computer. For backward compatibility with older computers using BIOS firmware, you can use disks with the [**Master Boot Record (MBR)**](javascript://) partition style. [Table 5-1](javascript://) summarizes the differences between GPT and MBR partition styles.

**Table 5-1**

### Disk Partition Styles

| **GPT** | **MBR** |
| --- | --- |
| Bootable only from UEFI firmware | Bootable from BIOS or UEFI firmware |
| Maximum 18 million TB (theoretical) | Maximum 2 TB usable space |
| Maximum 128 partitions | Maximum 4 partitions |

Like the older BIOS standard, UEFI firmware controls the startup process of the computer and eventually loads the operating system. New computers designed to run Windows 10 are sold with UEFI firmware. Computers with UEFI typically support the option of emulating legacy MBR-based boot firmware to run older operating systems; however, this reintroduces the legacy limitations of the MBR standard for device support. UEFI firmware that is up to date and running in full UEFI mode provides the best support for Windows 10 operation and management, including features that require UEFI firmware operating in full UEFI mode, such as Secure Boot, Device Guard, and Credential Guard.

Prior to Windows 10 Version 1703, the only way to upgrade an MBR partition to GPT was to back up the data, reinitialize the disk using MBR as GPT, then restore data from the backup. Windows 10 Version 1703 introduced the command-line tool [**MBR2GPT**](javascript://), which is designed to work offline in the recovery environment as part of the Windows boot upgrade process from BIOS/MBR to UEFI/GPT. It is important to note that even though MBR2GPT can be run from the regular Windows 10 environment, it is not recommended because misconfiguration issues can arise.

**Caution**

Before you use MBR2GPT on a boot disk, verify that the computer is using UEFI firmware.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-3**Disk Types

Empty space on disk drives can be identified by the type of storage using three different types in Windows 10: basic disks, dynamic disks, and Storage Spaces.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3aBasic Disks

When a new hard disk is added to a computer, it is initially configured as a [**basic disk**](javascript://). A basic disk can be partitioned using either MBR or GPT. Because basic disks have been in use for so long, many people and most computer utilities understand how to work with basic disks.

A basic disk is organized into one or more defined areas of storage called partitions. Each partition is identified by its size and the type of data it is supposed to hold. Most of these partition attributes are stored in a data table on the disk that is part of the MBR or GPT specifications. This table is commonly called the [**partition table**](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3bDynamic Disks

[**Dynamic disks**](javascript://) are an older technology that were introduced as an alternative to basic disks using an MBR partition style. A primary advantage of dynamic disks at the time was the ability to create many [**volumes**](javascript://) on a disk and avoid the MBR limitation of four partitions. On Dynamic disks, volumes provide similar functionality to partitions on basic disks. Dynamic disks also have support for distributing a volume over multiple hard drives, with or without fault tolerance.

**Note 2**

To simplify disk management terminology, many disk management utilities refer to partitions on basic disks as volumes.

The use of dynamic disks never really caught on and their use is not recommended for Windows 10. Microsoft recommends that the only reason to use dynamic disks with Windows 10 is for mirrored boot volumes. The advanced features and resilience enabled when using dynamic disks for data are now available in Storage Spaces.

**Tip**

If you need the advanced features and resilience available when using dynamic disks, use Storage Spaces instead.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-3cStorage Spaces

In Windows 10, the [**Storage Spaces**](javascript://) feature is an inexpensive way to combine, or pool, the storage of multiple physical disk drives. Storage Spaces can also provide fault tolerance with data redundancy across multiple disks. Implementing Storage Spaces is easier and less expensive than most consumer-level, hardware-based solutions for disk redundancy.

For disk pooling and fault tolerance, older operating systems typically relied on custom software or hardware-based RAID technology installed on the local computer, which could require expensive or proprietary mechanisms. Storage Spaces is a software-based storage technology that doesn’t need specialized storage hardware.

You can’t use Storage Spaces for the Windows 10 boot drive. So, to obtain any benefit from Storage Spaces, at least two extra drives are required, in addition to the drive where Windows was installed. Multiple disk technologies (e.g., SATA, SAS, USB) can be used at the same time. Storage Spaces can be configured to store multiple copies of data on more than one drive to mitigate the risk of a hard drive failure. Another benefit of using Storage Spaces as a software-based solution is that you can move Storage Spaces disks to another Windows 10 computer and still get access to the data.

**Caution**

Storage Spaces on Windows 10 is designed to work with common consumer-grade disk components. If a disk is attached to the computer using a RAID-based technology, it should not be used with Storage Spaces.

Storage Spaces technology combines selected individual disks into a managed logical group called a [**storage pool**](javascript://). The storage pool acts as a container for data storage and can grow or shrink as physical disks are added or removed from the pool. The storage pool, in turn, presents the user a portion of that space as a [**Storage Spaces volume**](javascript://)—a virtualized representation of a disk capable of storing the user’s files.

**Note 3**

The terms Storage Spaces volume and storage space are commonly used interchangeably to describe a volume hosted by Storage Spaces technology.

### Storage Pool

The first step in configuring Storage Spaces is creating a storage pool. You do this by identifying one or more disks that should be assigned to the pool. Once disks are assigned to a storage pool, Storage Spaces has access to the disks. More than one storage pool can reside on the same computer; however, a disk can be assigned to only one storage pool. Disks can be added and removed from a storage pool, making the storage technology flexible to the capacity needs of the user.

If a storage pool is running low on free drive space, you can add another disk to the computer while it is up and running and then assign it to the storage pool to increase its capacity. To accommodate this flexible technology, Microsoft designed Storage Spaces to work with a wide variety of disks at the same time. Some disk technologies are limited by the number of physical devices that can be added or by speed limitations built into those technologies (such as USB). Storage Spaces does not remove those limitations, but it allows multiple disks to be combined using different interface technologies simultaneously.

Disks can be removed from a storage pool if the remaining disks in the pool can store the information that was on the disk being removed. During the removal process, that disk has its data moved to the remaining disks in the pool. If the pool does not have enough space to hold that data, the disk removal fails.

**Caution**

When a disk is assigned to a storage pool, all its previous contents are erased. If desired, back up the contents before adding it to a storage pool.

The storage pool hides the details of the physical disks it combines into what appears as one large reservoir of storage. Users don’t interact directly with the storage pool and have no way of knowing which disks in the pool their data is stored on.

### Storage Space

After disks have been added to a storage pool, you need to allocate space from the pool for data storage. The space you allocate from the storage pool is called a storage space, otherwise known as a Storage Spaces volume. To users, a storage space is a single logical disk, but it can contain space from one or more disks that are members of the storage pool.

Storage Spaces technology allows for the overallocation, or overbooking, of storage spaces created from storage pools. The size of the storage pool does not restrict the specified maximum size of the storage space created from it. The maximum size of a storage space volume is a logical limit and can be larger than the storage pool disk capacity. For example, if a storage pool has 500 GB of capacity, a 900 GB storage space volume can be created from it without generating an error. This maximum volume size is a theoretical limit, not a measured quantity in this case.

The size of the physical storage pool does set a practical limit of how much actual data can be saved to a storage space volume. If the storage pool used to create a 900 GB volume has only 500 GB of physical disk space available, Windows 10 completes write operations to the volume without an issue as long as free space exists in the pool hosting that volume. As the available free space in the physical storage pool gets low, Windows warns users that they need to add more disks to the storage pool, delete some other data in the pool, or save less data to the pool.

The data written to a Storage Space volume is organized and spread by Windows 10 among the disk drives in the storage pool to maximize efficiency and redundancy in an automated fashion. All the disks that belong to a storage pool are known to one another as members of the same group. If one physical disk member fails, the storage space volumes created from the pool may fail or survive depending on how the volume was configured for resiliency.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-4**Disk Management Tools

Windows 10 includes multiple tools that you can use to manage disks. End users are typically most comfortable using the graphical Disk Management console. Administrators might use the command-line DiskPart utility or Windows PowerShell cmdlets for scripting.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

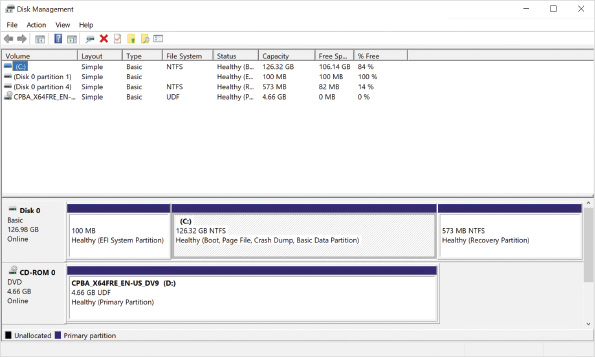
## 5-4aDisk Management Console

The [**Disk Management console**](javascript://) is an MMC snap-in (diskmgmt.msc) that is also part of the Computer Management utility. To use Disk Management and make changes to the disk configuration, you need to be a member of the Administrators group. Disks that are part of a storage pool are not visible in the Disk Management console, but Storage Spaces volumes are.

The Disk Management console allows changes to be made interactively and usually takes effect immediately without requiring the computer to be restarted.

As shown in [Figure 5-1](javascript://), the Disk Management console is divided into two views, a top view and a bottom view. The top view defaults to a summary of the volumes and partitions on the computer. The bottom view defaults to a graphical view of the disks and the volumes/partitions they contain.

**Figure 5-1Disk Management Console**



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4bDiskPart

[**DiskPart**](javascript://), shown in [Figure 5-2](javascript://), is a command-line tool that allows disk, partition, volume, and virtual hard disk management operations to be performed from a text-based screen interactively or from within a scripted file using command-line parameters.

**Figure 5-2DiskPart Running in Interactive Mode**



Enlarge Image

Operations in the DiskPart utility are driven by a sequence of commands. Each command must have a specific object on which to focus its action. For example, before a partition can be created, the DiskPart utility must be told which disk the partition will be created on. Items such as disks and partitions are usually numbered, with the first disk or partition object starting at 0. If you set the focus incorrectly, destructive operations can remove or delete data unexpectedly.

**Tip**

To see a list of DiskPart commands, type help at the DiskPart command prompt. To see more details about a specific DiskPart command, type help command\_name, where command\_name is the command of interest.

The DiskPart utility is powerful; it can contain a series of maintenance or repair commands that can be executed as part of a scheduled task or automated response on the local computer or remotely from another computer. It is considered an advanced tool that is not normally used for day-to-day administration. The tool can be run only in the security context of a user with local Administrator rights.

**Activity 5-1**

### Using DiskPart

**Time Required:**10 minutes

**Objective:**Start the DiskPart utility, browse its help menu, and use DiskPart to explore fundamental disk properties

**Description:**In this activity, you start the DiskPart utility, browse its help utility, and try out basic DiskPart commands.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, in the search box type **cmd**, and then click **Run as administrator** in the details pane.

1. 3

In the User Account Control dialog box, click **Yes**.

1. 4

Type **diskpart** and then press **Enter** to start the DiskPart utility in its interactive mode. Note that the prompt changes to DISKPART>.

1. 5

Type **help** and then press **Enter** to see a list of DiskPart commands.

1. 6

Type **help select** and then press **Enter** to see information about the select command.

1. 7

Type **help select disk** and then press **Enter** to see information and examples for the select disk command.

1. 8

To see what disks can be selected, type **list disk** and then press **Enter**.

1. 9

The DiskPart utility has not been focused on a particular disk yet, so some commands will not be able to run. For example, type **list partition**, press **Enter**, and note the error message.

1. 10

To focus attention on the first disk, type **select disk = 0** and then press **Enter**.

1. 11

Type **list partition**, press **Enter**, and note that the error message is gone.

1. 12

To see what volumes are visible to the DiskPart utility, type **list volume** and then press **Enter**.

1. 13

To leave the DiskPart utility, type **exit** and then press **Enter**.

1. 14

Close the Administrator: Command Prompt window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-4cStorage Cmdlets in Windows PowerShell

Windows PowerShell cmdlets can be used to manage the Windows 10 storage subsystem, including Storage Spaces. Using Windows PowerShell cmdlets to manage storage avoids the quirks and older syntax of the DiskPart utility.

One advantage of using storage cmdlets in PowerShell is that configuration steps can be deployed without clicking around in the graphical consoles. This is very useful in more complicated server environments, such as virtual servers or cloud computing, but it can also be used in the Windows 10 environment for advanced management, automation, and troubleshooting.

**Activity 5-2**

### Use Windows PowerShell to Manage Storage

**Time Required:**10 minutes

**Objective:**Use Windows PowerShell to view basic storage properties for disks, volumes, and partitions.

**Description:**In this activity, you view the storage cmdlets available in Windows PowerShell and then use them to view storage information.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 3

In the User Account Control dialog box, click **Yes**.

1. 4

Type **Get-Command -Module Storage** and then press **Enter**. This lists all the cmdlets available in the currently installed Windows Storage module.

1. 5

At the Windows PowerShell prompt, type **Get-Disk** and then press **Enter**. This lists all physical disk objects, like basic disks, organized in a table.

1. 6

Type **Get-Disk | FL Number, FriendlyName, PartitionStyle, BusType** and then press **Enter**. This lists specific attributes for each drive, including some additional information that was not shown in the default table format. Note that not all data returned by a straightforward PowerShell command like Get-Disk is displayed on the screen by default.

1. 7

Type **Get-Partition** and then press **Enter**. This shows all the partitions, organized by disk, even if they are not formatted as a volume to store files.

1. 8

Type **Get-Volume** and then press **Enter**. This returns a table of all volumes on all partitions for all disks.

1. 9

Type **Get-Volume | Where-Object {$\_.DriveLetter -ne $null}** and then press **Enter**. This shows the power of PowerShell to generate a filtered view, in this case only the volumes that have a drive letter assigned.

1. 10

Close the Windows PowerShell prompt window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-5**Managing Physical Disks

When you have a computer with a single hard drive, that hard drive is prepared for use during the installation of Windows 10. On a computer that already has Windows 10 installed, you might add one or more hard drives for additional storage. When you add a hard drive that’s connected internally, it’s typically connected via SATA. When you connect a hard drive externally, it’s typically connected via USB.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-5aAdding a New Drive

When you add a new SATA drive, it is connected to cabling inside your computer when the computer is turned off. When you restart the computer, it needs to be identified by the firmware in your computer and then Windows 10 has access to the drive. If a newly connected SATA drive is not visible in Disk Management, then you should verify that the SATA port is enabled in firmware. Even though it is common for computers to have multiple SATA ports, manufacturers often only enable the SATA ports with devices connected.

When you add a new USB drive, it is connected to an external USB port when the computer is turned on. Plug and Play functionality in Windows 10 detects the new USB drive, loads the appropriate drivers, and then Windows 10 has access to the drive. In rare cases, a USB drive requires unique drivers not included in Windows 10 and you need to install the appropriate drivers. You might need to go into Device Manager and scan for new hardware changes for the embedded storage controller to be detected properly.

Sometimes Plug and Play doesn’t identify new drives properly even when the storage driver is loaded. In many cases, it is easiest to restart the computer and then the drive is usually detected properly. Alternatively, you can use Disk Manager and scan for new disks to trigger the discovery process. If a new disk appears in Disk Manager but is offline, you can bring it online in Disk Manager. You can also bring a disk online by using the Set-Disk cmdlet.

Most new hard disks can’t be used to store files until you [**initialize**](javascript://) them with the MBR or GPT partition style. When you initialize a disk, it applies the selected partition style and marks the disk with a digital signature that Windows 10 can use for identification. Some new hard disks are initialized by the manufacturer.

**Tip**

If you are adding a new disk to a storage pool, then you don’t need to initialize it.

In Disk Management, a new disk that is not initialized has a status of Unknown. If necessary, you can trigger the disk initialization process manually in Disk Management or by using the Initialize-Disk cmdlet. Disk Management prompts you for the partition style. You can specify a partition style when using Initialize-Disk, but if you don’t specify a partition style then GPT is used by default.

**Caution**

If you initialize a disk that already has data on it, that data is erased.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-5bMoving Drives

There are no special considerations for moving basic disks. When you move a basic disk to another computer, all the data on the disk is available in the new computer, but the drive letters assigned to each volume might be changed.

If you move a dynamic disk to another computer, you need to import it. Before the disk is imported, the Disk Management console reports the status of the disk as a [**Foreign Disk**](javascript://) and you don’t have access to data on the disk. You must right-click the disk name in Disk Management and then select Import Foreign Disk to initiate the import process.

If a dynamic disk contains a volume that is spread across multiple dynamic disks, all member disks must be moved at the same time. Failure to do so leaves the volume broken, even if the dynamic disk is correctly imported.

Storage Spaces technology is similar to dynamic disk technology in that it keeps track of each disk that is a member of a storage pool. When a storage pool is moved from one computer to another, all disk members of the pool should be moved at the same time. Once the disks are connected to the target Windows 10 computer, the pool and its Storage Spaces volumes mount automatically as read-write storage.

**Caution**

Moving multiple disks between computers is always risky. If the data is important, back up the data at the source before the move as a precaution.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-6**Virtual Disk Management Tasks

Windows 10 provides native support for working with VHDs. Disk Management and DiskPart are automatically available for creating and managing VHDs. The Windows PowerShell cmdlets for managing VHDs are installed as part of the Hyper-V Module for Windows PowerShell feature. If you have installed Hyper-V on the computer, this module is included by default. Otherwise, you can install the module by itself as an additional feature.

**Tip**

Windows 10 Home edition does not include the Hyper-V Module for Windows PowerShell.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-6aCreating VHDs

A VHD in Windows 10 is created as a single file on a physical disk drive. All versions of Windows 10 support the capability to create a VHD. VHDs can be created using the Disk Management snap-in, the New-VHD cmdlet, or the DiskPart command-line utility.

To create a VHD, you must specify the following information:

* Location—This includes the name and physical location of the file that will hold the VHD data. The location needs to be large enough to hold the VHD file and all its data.
* Virtual Hard Disk Format—This specifies VHD or VHDX. VHD is an older format that supports virtual disks up to 2 TB. VHDX is a newer format that supports virtual disks up to 64 TB and has better performance.
* Virtual Hard Disk Size—This states a maximum storage limit specified in MB, GB, or TB.
* Virtual Hard Disk Type—This specifies whether the type is dynamically expanding or fixed size. A dynamically expanding VHD takes up only the disk space required to hold the data inside it and has a maximum size allocated. A dynamically expanding VHD behaves much like a compressed folder (.zip) that expands as you add content to it. A fixed-size VHD immediately takes up the full size allocated to the VHD.

VHD disks created by using Disk Management automatically attach to the operating system and appear as a new disk drive that is uninitialized. The drive must be initialized, just like a new hard drive, before it can be configured with partitions to store files. VHDs are restricted to basic disk technology due to their transient existence in the operating system.

**Caution**

Because VHDs are not automatically reattached after signing out, shutting down, or restarting, you should not sign out, shut down, or restart during an activity that involves a VHD unless instructed otherwise.

**Activity 5-3**

### Creating VHD Disks

**Time Required:**10 minutes

**Objective:**Create a new VHD disk

**Description:**In this activity, you perform the typical steps required to create a new VHD disk hosted on drive C:.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then select **File Explorer**.

1. 3

Click to select **Local Disk (C:)** in the left-pane and create a new folder in the root of C: called **VHD Storage**.

1. 4

Right-click the **Start** button and then select **Disk Management**.

1. 5

In the Disk Management window, click **Disk 0**, click **Action** on the menu bar, and then select **Create VHD**. This displays the Create and Attach Virtual Hard Disk dialog box.

1. 6

Click the **Browse** button and navigate to **C:\VHD Storage**. In the File name field, enter the text **VHDExample** and then click the **Save** button.

1. 7

In the Create and Attach Virtual Hard Disk dialog box, in the Virtual hard disk size, type **5**, and then change the unit size to **GB**.

1. 8

In the Virtual hard disk format area, click **VHDX**.

1. 9

In the Virtual hard disk type area, verify that **Dynamically expanding** is selected.

1. 10

Click **OK** to create the VHD and automatically attach it.

1. 11

Note that a new disk appears in the graphical disk view with an Unknown disk type and a status of Not Initialized. The free space on the drive appears as 5 GB of unallocated space and the graphical drive icon next to the disk identifier is light blue.

1. 12

Right-click anywhere within the 5 GB block of unallocated space shown as part of the newly created VHD disk, and note the available volume creation options are all dimmed and unavailable.

1. 13

Right-click the VHD’s disk name next to the blue drive icon and then select **Initialize Disk** on the shortcut menu.

1. 14

In the Initialize Disk dialog box, select **MBR** and then click **OK**.

1. 15

Right-click the unallocated space from the VHD disk and then select **New Simple Volume**.

1. 16

When the first wizard screen is displayed, click **Next**.

1. 17

On the Specify Volume Size screen, click **Next** to accept the suggested volume size.

1. 18

On the Assign Drive Letter or Path screen, note the drive letter assigned to the new simple volume and then click **Next**.

1. 19

On the Format Partition screen, in the Volume label box, type **VHDVOL**, click **Next**, and then click **Finish**.

**Note 4**

During the creation and formatting of the drive, Windows might mistakenly prompt you to format the new volume even though the wizard is performing that task for you. If that happens, just click **Cancel** at the prompt asking Do you want to format it?

1. 20

Note the size of the newly created partition in Disk Management. It is reported as the full size of 5 GB you specified in the New Volume Creation Wizard.

1. 21

Switch to the File Explorer window and browse to **C:\VHD Storage**. Note the size of the VHD file in that folder and the fact that it is much smaller than the reported volume size.

1. 22

In the File Explorer window, right-click the drive letter assigned to the VHD disk and select **Properties**. Note the Used Space and Free Space values shown on the General tab. Compare this with the actual size of the VHD file noted in the previous step.

1. 23

Click **OK** to close the drive Properties dialog box.

1. 24

Close all open windows, but do not sign out or restart.

**Caution**

[Activity 5-4](javascript://) relies on the VHD created and mounted in [Activity 5-3](javascript://). Do not sign out, restart, or shutdown between [Activity 5-3](javascript://) and [Activity 5-4](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-6bAttaching and Detaching VHDs

A VHD must be attached, or mounted, to be available to the operating system and the user. When a VHD is attached, it can be managed with typical disk and partition operations. All versions of Windows 10 can attach an existing VHD file. VHDs can easily be attached by double-clicking the VHD file name in File Explorer.

VHDs can also be attached using methods that offer more control, such as the Mount-VHD cmdlet, Disk Management, or the DiskPart command-line utility. When a VHD file is attached via these methods, it can optionally be opened in read-only mode where its file contents cannot be accidentally modified.

When a Windows 10 computer is restarted, the VHD files currently attached do not automatically reattach. They must be manually attached again after the computer restarts. The only time a VHD automatically mounts as the computer starts is the special case in which Windows 10 is configured to boot from a VHD file.

A VHD must be detached, or dismounted, to make it unavailable to the operating system and the user. All versions of Windows 10 support the capability to detach an existing VHD file. VHDs can be detached using the Disk Management snap-in, the Dismount-VHD PowerShell command, or the DiskPart command-line utility.

**Activity 5-4**

### Managing VHD Disks

**Time Required:**5 minutes

**Objective:**View VHD attributes using DiskPart and detach a VHD

**Description:**In this activity, you use DiskPart to view a VHD’s details, detach it, and confirm that it is no longer visible as an active disk.

1. 1

Right-click the **Start** button and then click **File Explorer**.

1. 2

Confirm that you can see the drive letter associated with the VHD created and mounted in [Activity 5-3](javascript://).

1. 3

Click the **Start** button, in the search box type **cmd**, right-click the result **Command Prompt**, and then click **Run as administrator** on the shortcut menu.

1. 4

In the User Account Control dialog box, click **Yes**.

1. 5

At the command prompt, type **diskpart** and then press **Enter**.

1. 6

To focus attention on the VHD created in the previous activity, type **select vdisk file= “C:\VHD Storage\VHDExample.vhdx”** and then press **Enter**.

1. 7

Type **detail vdisk** and then press **Enter** to display detailed information about the VHD. Note the Virtual size and Physical size attributes listed in the output of the command.

1. 8

Type **detach vdisk** and then press **Enter** to dismount the VHD.

1. 9

Type **exit** and then press **Enter** to exit DiskPart.

1. 10

Switch to the File Explorer window. Confirm that you can no longer see the drive letter associated with the VHD created and mounted in [Activity 5-3](javascript://).

1. 11

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-7**Managing Storage Spaces

Management of Storage Spaces is not integrated into Disk Management or DiskPart. A new graphical control interface called Manage Storage Spaces is found in the System and Security section of Control Panel. This tool allows administrative users to create and manage storage pools and storage spaces.

Manage Storage Spaces allows changes to be made interactively and take effect immediately without requiring the computer to be restarted. Physical disks that are added to storage pools can be managed with the Disk Management console before they are added to a storage pool, but once they are added to a storage pool, they must be managed within the Manage Storage Spaces view.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-7aCreating an Initial Storage Pool and Storage Space

Initially, Manage Storage Spaces shows only a link to create a new storage pool and storage space.

If no disks exist except for the system disk (i.e., drive C:), the Storage Spaces wizard notifies the user that no drives are available for use with the technology. Before a storage pool can be created, at least one additional drive must be added to the computer and must be recognized by the system. Once a storage pool exists, the Manage Storage Spaces view changes to provide management options for existing storage pools and storage spaces, as shown in [Figure 5-3](javascript://).

**Figure 5-3Storage Space Settings after the Initial Setup**



Enlarge Image

**Caution**

[Activity 5-6](javascript://) relies on a VHD that is mounted in [Activity 5-5](javascript://). Do not shut down, restart, or sign out between [Activity 5-5](javascript://) and [5-6](javascript://).

**Activity 5-5**

### Creating the Initial Storage Pool and Storage Space Volume

**Time Required:**15 minutes

**Objective:**Create a storage pool and storage space volume using the initial Storage Spaces Wizard

**Description:**In this activity, you create a new virtual disk that is attached and empty. Using PowerShell, you create a new storage space pool and volume from that virtual disk. Finally, you confirm the storage space volume’s settings in the Disk Management console to note key information.

**Caution**

VHDs are not officially supported for Microsoft Storage Spaces because they do not automatically remount in Windows 10. They are used in this lab only to illustrate Storage Spaces concepts and should never be used in a production environment with Storage Spaces. Because of their unsupported nature, we will use the precision of PowerShell commands to build our Storage Spaces environment.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Disk Management**.

1. 3

In the Disk Management window, click **Action** on the menu bar and then click **Create VHD**.

1. 4

In the Create and Attach Virtual Hard Disk dialog box, click the **Browse** button and navigate to the location **C:\VHD Storage**, which was created in [Activity 5-3](javascript://).

1. 5

In the File name box, type **VHDPoolDisk1** and then click **Save**.

1. 6

In the Virtual hard disk size box, type **7** and then change the unit size to **GB**.

1. 7

Confirm that **VHD** is the virtual hard disk format selected.

1. 8

In the Virtual hard disk type area, select **Dynamically expanding** and then click **OK**. Note that the disk appears in Disk Management as an uninitialized disk with 7 GB of unallocated space.

1. 9

Click the **Start** button, in the search box type **control panel**, and then click **Control Panel**.

1. 10

Click **System and Security** and then click **Storage Spaces**.

1. 11

Click the **Create a new pool and storage space** link. When you are prompted by User Account Control for permission to run the application, click **Yes**.

1. 12

Note that the Storage Spaces agent has discovered the newly created and attached VHD as an available disk and has already selected it by default. Click **Create pool**.

1. 13

In the Create a storage space window, enter the following information and then click **Create storage space**.

* + Name: **Simple space**
  + Drive letter: **D:**
  + File system: **NTFS**
  + Resiliency type: **Simple (no resiliency**)
  + Size (maximum): **10 GB**

1. 14

In the Storage Spaces window, expand **Physical drives**. Read the information displayed to see information about the storage space and the physical drives it is located on.

1. 15

Switch to the Disk Management window and note that the VHD is no longer displayed as a disk visible to Disk Management. Instead, you can see a new basic disk with a volume named Simple space. Simple space is the storage space that you created.

1. 16

Right-click the newly created disk name and then select **Properties**.

1. 17

Click to select the **General** tab if it is not selected. Note that the Location is specified as on Microsoft Storage Spaces Controller.

1. 18

Click to select the **Volumes** tab. Note that the default partition style was defaulted to GUID PartitionTable (GPT).

1. 19

Click **OK** to close the Microsoft Storage Spaces Device Properties window.

1. 20

Right-click the **Start** button and then select **File Explorer**.

1. 21

Navigate to the folder **C:\Program Files**, right-click the **Common Files** folder and then click **Copy**.

1. 22

Navigate to the drive letter for the Simple space volume and paste the Common Files folder. This content is used to provide some data within the storage space volume for later activities.

1. 23

Close all windows but do not sign out or restart your computer.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-7bMaintaining Storage Pools and Storage Spaces

Each storage pool is identified by the physical disk members that are grouped within that pool. Metadata about the pool and its members is stored on each physical disk that is a member of the pool. The end user has the option to customize a storage pool by:

* Renaming a storage pool—The default name for the first storage pool is just the name Storage pool. If you intend to have multiple storage pools, it might be desirable to rename this pool based on some attribute of the data or disks that are contained within the pool.
* Adding disk drives to the pool—You can add more disks to the storage pool after the disk is connected to the computer and visible to Windows 10. The physical disk must be at least 4 GB in size; if it is smaller, Storage Spaces does not allow that disk to be selected. If the disk contains any previous data, it is destroyed once the disk is joined to a storage pool.
* Creating or deleting a storage space volume assigned to the pool—The maximum size of a volume created from the storage pool is not limited by the storage pool, and similarly, the number of volumes created from one storage pool is not limited by just having one storage pool. The biggest limitation to the number of storage space volumes is the availability of free drive letters to assign to those volumes.
* Optimizing drive usage within the pool—When data is written to a storage pool, Windows 10 manages the placement of the data on the physical disks. As physical disks are assigned to the pool, Windows by default tries to rebalance the data across all the disks that belong to the pool. If a storage pool was created with an earlier version of Windows and upgraded for use with Windows 10, or automatic rebalancing was not enabled when a disk was added to a storage pool, you can manually trigger the optimization and rebalancing of data across all drives in the pool as a background activity.

**Activity 5-6**

### Managing Storage Pools and Storage Space Volumes

**Time Required:**20 minutes

**Objective:**Investigate options to manage a storage pool and storage space volumes using the Storage Spaces section in Control Panel

**Description:**In this activity, you rename the storage pool to aid the end user’s recognition of the storage pool, plus look at the option to add a second virtual disk to the existing storage pool. The activity looks at the options to create a new simple storage volume.

1. 1

You should already be signed in from the previous activity.

1. 2

Right-click the **Start** button and then select **Disk Management**.

1. 3

In the Disk Management window, click **Action** on the menu bar and then click **Create VHD**.

1. 4

In the Create and Attach Virtual Hard Disk window, click the **Browse** button and navigate to the location **C:\VHD Storage**. In the File name box type **VHDPoolDisk2** and then click **Save**.

1. 5

In the Virtual hard disk size box, type **6** and then change the unit size to **GB**.

1. 6

Confirm that VHD is the virtual hard disk format selected.

1. 7

In the Virtual hard disk type area, select **Dynamically expanding** and then click **OK**.

1. 8

Click the Start button, type **storage**, and then click **Manage Storage Spaces**.

1. 9

Click the **Change settings** button.

1. 10

When you are prompted by a User Account Control dialog box for permission to run the application, click **Yes**. Note that the links to manage the existing storage pool and its storage spaces are now active.

1. 11

Click the **Rename pool** link.

1. 12

In the Name box, type **Archive Storage** and then click **Rename pool**.

1. 13

Click the **Add drives** link.

1. 14

Note that a list of available unformatted drives is presented in the Add drives wizard. Confirm that the **Optimize drive usage to spread existing data across all drives** option is selected.

1. 15

Confirm that the virtual disk added earlier in the activity is selected and then click **Add drives**.

1. 16

In the Storage Spaces window, in the Archive Storage area, expand Physical Disks. Note that two disks are shown.

1. 17

Click the **Optimize drive usage** link and then click the **Optimize drive usage** link button to trigger the process manually. Optimization is a background task that will proceed until it completes.

1. 18

Click the link **Create storage space**.

1. 19

In the Name and drive letter settings area, in the Name box, type **STORVOL2**.

1. 20

In the Resiliency area, in the Resiliency type box, select **Simple (no resiliency)**.

1. 21

In the Size area, in the Size (maximum) box, type **20 GB** and then click **Create storage space**.

1. 22

Close all windows and sign out.

**Note 5**

After this activity, you can shut down, restart, or sign out.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-7cConfiguring Storage Spaces Fault Tolerance

Individual physical disks configured as basic disks are not fault tolerant themselves. If the data is not backed up, the loss of a basic disk results in permanent data loss.

**Note 6**

This module provides disk fault-tolerance information specific to Windows 10 and Storage Spaces. If you would like to review generic RAID fault tolerance, please see Standard RAID levels on Wikipedia at [https://en.wikipedia.org/wiki/Standard\_RAID\_levels](https://en.wikipedia.org/wiki/Standard_RAID_levels" \t "_blank).

A storage space volume can be configured for fault tolerance when it is initially created if the proper starting conditions are met. Individual drives within the storage pool are used by Windows 10 transparently to provide the level of fault tolerance requested. Different levels of fault tolerance are available that are similar to traditional RAID levels but are customized to operate with additional functionality not normally found in traditional RAID. These fault-tolerant options are listed in [Table 5-2](javascript://).

**Table 5-2**

### Storage Spaces Resiliency Types

| **Resiliency Types** | **Description** |
| --- | --- |
| Simple (no resilience) | - Needs one drive minimum in the pool  - Good for temporary data and where performance is more important than resilience  - If a drive in the pool fails and contains part of this volume, the volume is not available to the end user |
| Two-way mirror | - Needs two drives minimum  - A volume’s data is copied to at least two separate disks in the pool; each disk holds a synchronized copy of the volume’s data  - Good performance with disk read and write operations  - Can handle a single drive failure and still be operational  - Supported volume size is limited to the size of the smallest drive member |
| Three-way mirror | - Needs five drives minimum  - Three copies of a volume’s data are spread across all five drives  - Good performance with disk read and write operations  - Can handle multiple drive failures and still be operational |
| Parity | - Similar to RAID 5 in that parity information is calculated and can determine data that is lost from a drive failure  - Needs three drives minimum to handle a single drive failure  - Needs seven drives minimum to handle a double drive failure  - Slow performance during a disk failure while the system calculates missing data; best used for low data that needs fault tolerance but not high performance, such as archive data |

Enlarge Table

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-8**File Systems

Once a volume is available to store data, its free space must be organized into files and folders using a file system. A user typically has different file storage requirements for different devices. For example, some files must be portable and interchangeable with other operating systems, while other files must be secure and efficiently stored. Some devices, such as hard disks, support multiple file systems on one device. This section discusses the common file systems used in Windows 10, the properties of files stored on them, and securing those files.

A file system allows the operating system to store and organize files. The choice of file system can limit the total amount of data stored in a partition or volume, the number of files, the size of the files, their names, attributes, and other properties. Windows 10 supports several common file systems:

* File Allocation Table (FAT)
* NT File System (NTFS)
* Resilient File System (ReFS)
* Universal Disk Format (UDF)

**Note 7**

The choice of basic or dynamic disk technology has no impact on the system features described in this section.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-8aFile Allocation Table (FAT)

The earliest file system used for hard disks by the MS-DOS operating system is the [**File Allocation Table (FAT)**](javascript://). All Microsoft operating systems since MS-DOS support a version of this file system. Different versions of FAT can be used with Windows 10: FAT, FAT32, and exFAT.

FAT is a simple and basic method to organize files on partitions that are no larger than 4 GB in size. FAT32 was introduced with Windows 95 OSR2 to support hard disks that were becoming much larger than 2 GB in size. Windows 10 does not use FAT32 as a file system for new partitions or volumes larger than 32 GB.

Microsoft introduced exFAT with Windows Vista Service Pack 1 and continues to license the technology to memory device manufacturers, such as USB memory sticks. ExFAT has the simplicity of the FAT file system but with capacity limits that are so large that it can be used with almost any portable bulk storage device. As memory device sizes exceed 32 GB, exFAT could be the file system of devices preformatted at the factory.

**Note 8**

A volume can’t be formatted with exFAT using graphical tools; however, the format K: /FS:exFAT command formats the specified volume, K:, with the exFAT file system from the command line. The format utility supports the FS (i.e., file system) parameters FAT, FAT32, exFAT, NTFS, UDF, ReFS.

In Windows 10, FAT should be used for file systems only when portability to non-Microsoft operating systems is a concern. Generally, this means that FAT is used only for portable media such as USB memory sticks and memory cards for phones and digital cameras. FAT does not provide file system security. To provide enhanced features for security, usability, and larger partitions, NTFS is a better alternative.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-8bNew Technology File System (NTFS)

The [**New Technology File System (NTFS)**](javascript://) was first introduced with Windows NT, and a newer version of it is supported by Windows 10. NTFS stores files and folders in a way that looks very similar to the FAT file system. The difference is in how that data is secured, reliably managed, and allowed to grow. The major advantages of NTFS are listed in [Table 5-3](javascript://).

**Table 5-3**

### Advantages of the NTFS File System over FAT

| **Advantage** | **Description** |
| --- | --- |
| File and Folder permissions | Each file and folder has its own discretionary access control list (DACL) of who (i.e., user or group) can do what to the file system object. Permissions include configurable inheritance through the folder structure. Permissions can be basic or advanced using allow or deny assignments. Ownership of a file system object is tracked and always allows access to file system objects owned by that user or group. |
| Audit controls | Each file and folder can have its own custom system access control list (SACL) to define who is audited in the Security event log when they succeed or fail at accessing a file system object. |
| Compression | Files can optionally have their contents compressed. |
| Encrypting File System (EFS) | Files can optionally have their contents encrypted. |
| Disk quotas | Optionally track how much data is used on the file system by a user and potentially apply storage limits. |
| Automatic bad cluster management | Bad clusters that fail to store data reliably are tracked and not reused. |
| File names in Unicode format | File and folder names can contain international languages and symbols, not just ASCII characters. |
| Alternate data streams | Support for multiple data streams that link to the same file but have different purposes (e.g., file data for one stream, a bitmap in another stream for the app that is registered to open that type of file). |
| Transactional NTFS | This is used to protect data files with log files and checkpoint consistency checks. |
| Log file and checkpoint consistency checks | Changes made to key files can be rolled back in the event of a problem to a known good state. |
| Extendable/shrinkable partitions and volumes | As long as free space allows on the disk or volume, the partition or volumes can be extended or shrunk. |
| Volume mount points | You can link an empty folder in one volume to another volume. |
| Symbolic links | A symbolic link points to another file or folder, similar to a shortcut. To the user or application, it appears as if the file is in that folder. |

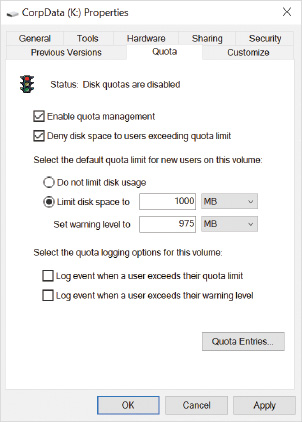
Enlarge Table

### Disk Quotas

[**Disk quotas**](javascript://) are primarily used on file servers to limit or monitor the amount of storage consumed by specific users. The ability to configure disk quotas is included as part of the NTFS files system, but it is seldom implemented on a computer running Windows 10. If you decide to implement quotas, you can do so on the Quotas tab in the Properties of a volume via File Explorer or Disk Management. You can also use the **[fsutil](javascript://)** command-line utility.

The Quota tab displays quota settings for that partition or volume, as shown in [Figure 5-4](javascript://).

**Figure 5-4NTFS-Formatted Disk Properties, Disk Quota Tab**



Once disk quotas are enabled for a partition, the operating system calculates the amount of disk space used by each unique owner listed for all files on the volume. The first time quota management is turned on, the system takes some time to identify all the owners and tally all the file sizes attributed to each owner. If the owner of a file changes, then the size of that file is applied to the quota of the new owner.

**Note 9**

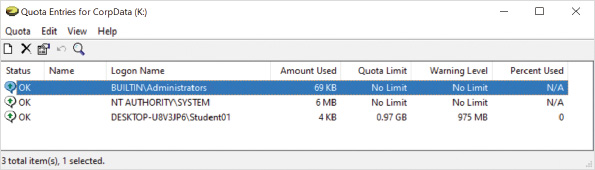
Compressed files count against the user’s quota based on their uncompressed size, not the compressed size.

Even if disk quotas are enabled, the initial configuration reports only the amount of data in use by different owners; no limits or warnings are enforced. The options on the Quota tab allow for limits to be configured as a default setting for all users.

As users approach those limits, warnings can be issued; when they finally reach the maximum limit, they are denied additional disk space within the partition. Warnings to users can be ignored, misinterpreted, and not noticed, so the warnings can be optionally recorded to the application event log as a permanent reference of the event for administrators.

Some users may require special consideration and should have a different warning or deny limit in place. The Quota Entries button on the Quota tab opens a Quota Entries window where user-specific limits can be defined that override the default settings. The Quota Entries window is shown in [Figure 5-5](javascript://).

**Figure 5-5Quota Entries for an NTFS-Formatted Disk**



Enlarge Image

**Caution**

[Activity 5-7](javascript://) relies on a VHD that is mounted. Do not shut down, restart, or sign out during this activity.

**Activity 5-7**

### Enabling Disk Quotas for an NTFS Partition

**Time Required:**15 minutes

**Objective:**Enable disk quotas

**Description:**Disk quotas can be used to limit disk utilization, but they can also be used just to identify the amount of disk space that each user is using. For example, if you enable quotas on the C: drive of a computer running Windows 10, you can see how much application data and profile space is used. In this activity, you enable disk quotas on the C: drive of your computer and log events when limits are reached.

1. 1

If necessary, start your computer and sign in.

**Note 10**

This activity uses a VHD created earlier in [Activity 5-3](javascript://).

1. 2

On the taskbar, click **File Explorer** and browse to **C:\VHD Storage.**

1. 3

To attach the VHD, right-click the **VHDExample.vhdx** file and then click **Mount**. Note the drive letter it was mounted as in relation to This PC.

1. 4

Right-click **VHDVOL (driveletter)** and then click **Properties**.

1. 5

In the VHDVOL (driveletter) Properties dialog box, click the **Quota** tab and then click the **Show Quota Settings** button. Note that the traffic light indicator on the Quota tab is red and that the status is reported as Disk quotas are disabled.

1. 6

Select the **Enable quota management** check box and then click **Limit disk space to**.

1. 7

In the Limit disk space to box, type **2** in the numeric field and then select **GB** in the units list.

1. 8

In the Set warning level to box, check that **1** is entered in the numeric field and select GB from the units list.

1. 9

Select the **Log event when a user exceeds their quota limit** and **Log event when a user exceeds their warning level** check boxes and then click **Apply**.

1. 10

A warning appears that enabling the disk quota system will take some time to complete. Click **OK** in the warning window to continue.

1. 11

When the traffic light indicator on the Quota tab turns green and the status is reported as Disk quota system is active, click the **Quota Entries** button.

1. 12

The Quota Entries for VHDVOL (driveletter) window dialog box displays and lists the current owners who have files on the volume. On slower systems, the Logon Name column is initially populated with the security identifiers (SIDs) of the owners found on the volume which is later updated to the friendly names.

1. 13

Click the **Start** button, in the search box type **cmd**, right-click the result **Command Prompt**, and then click **Run as administrator** on the shortcut menu.

1. 14

In the User Account Control dialog box, click **Yes**.

1. 15

Using the drive letter you noted in [Step 2](javascript://), at the command prompt, type **fsutil quota query** drive-letter (for example, fsutil quota query e:) and then press **Enter**. Note the detail reported in the text output by the command in comparison to the detail visible in the Quota Entries for (C:) dialog box displayed in [Step 12](javascript://). Consider which report could be generated by a scheduled task for routine reporting.

1. 16

Close all open windows and dialog boxes.

**Caution**

[Activity 5-8](javascript://) relies on a VHD that is mounted in [Activity 5-7](javascript://). Do not shut down, restart, or sign out between [Activity 5-7](javascript://) and [5-8](javascript://).

### Volume Mount Points

A partition or volume has a finite amount of space available. The partition or volume can be extended or spanned, but in some cases, this is not an option. [**Volume mount points**](javascript://) allow an empty folder in an NTFS-formatted file system to point to another partition or volume in the local computer. You can configure volume mount points by using the Disk Management console. The user performing the task must have administrator privileges on the local computer.

To the users, it appears they are accessing a folder in the original NTFS partition, but in fact they are accessing the file system on the other partition. The partition connected via the volume mount point can be formatted with a different file system. The disk space reported for the NTFS volume hosting the mount point does not increase; the volume mount point is just a pointer. The free space and control of the target pointed at by the volume mount point is separately reported and managed.

A folder must be empty before it can be converted into a volume mount point. A single volume mount point can only point to one partition or volume; however, multiple mount points can point to the same target partition or volume. Volume mount points can be added or removed for a partition, but they cannot be modified. If a partition or volume is deleted and it is pointed to by one or more mount points, those mount points will appear as broken links and will not revert to empty folders.

**Caution**

[Activity 5-8](javascript://) relies on a VHD that is mounted. Do not shut down, restart, or sign out during this activity.

**Activity 5-8**

### Managing Mount Points

**Time Required:**15 minutes

**Objective:**Link additional space to an existing volume using a volume mount point and observe the changes to the view in File Explorer

**Description:**You can use a mount point to expand the capacity of an existing partition or volume. This can be useful when you need to add a large amount of storage space and no space is available on the physical disk. For example, you can create a mount point for application data. In this activity, you create a mount point on the C: drive to hold data for an application.

1. 1

You should already be signed in from the previous activity.

1. 2

On the taskbar, click **File Explorer** and browse to C:\.

1. 3

In File Explorer, on the **Home** tab, click **New folder**, type **MyAppData**, and then press **Enter**.

1. 4

Browse to VHDVOL, click the **Home** tab, click **New item**, and click **Text Document**.

1. 5

Type **DataFile** and then press **Enter** to name the file.

1. 6

Close the File Explorer window.

1. 7

Right-click the **Start** button and then click **Disk Management**.

1. 8

Right-click **VHDVOL** (**driveletter:)** and then click **Change Drive Letter and Paths**.

1. 9

In the Change Drive Letter and Paths for driveletter: (VHDVOL) dialog box, select the drive letter and then click **Remove**.

1. 10

In the Disk Management window, click **Yes** to acknowledge the warning.

1. 11

Right-click **VHDVOL** and click **Change Drive Letter and Paths**.

1. 12

In the Change Drive Letter and Paths for VHDVOL dialog box, click **Add**.

1. 13

In the Add Drive Letter or Path dialog box, click **Mount in the following empty NTFS folder**, type **C:\MyAppData** in the text box, and then click **OK**.

1. 14

On the taskbar, click **File Explorer** and browse to C:\. Notice that MyAppData is displayed with a different icon and shows a size.

1. 15

Close File Explorer.

1. 16

Click the **Start** button, in the search box type **cmd**, right-click the result **Command Prompt**, and then click **Run as administrator** on the shortcut menu.

1. 17

In the User Account Control dialog box, click **Yes**.

1. 18

At the command prompt, type **dir C:\my\*** and then press **Enter**. Notice that MyAppData is identified as a junction point.

1. 19

Type **cd \MyAppData** and then press **Enter**.

1. 20

Type **dir** and then press **Enter**. Verify that DataFile.txt is there.

1. 21

Close the command prompt window.

1. 22

In Disk Management, scroll down in the list of disks, right-click the disk containing VHDVOL, and then click **Detach VHD** on the shortcut menu.

1. 23

In the Detach Virtual Hard Disk dialog box, click **OK**.

1. 24

Close the Disk Management window.

### Symbolic Links

A [**symbolic link**](javascript://) can point to a file or folder on the local computer or to a remote location identified with a UNC path. If the target is remote, the other computer hosting the target must also support symbolic links. The two special types of symbolic links are known as hard links and junction points. Only administrators can create symbolic links using the command-line utility **[mklink](javascript://)**.

Symbolic links are different from a shortcut because a shortcut is a file that defines how Windows can locate content somewhere else. To other applications, the shortcut appears as just another file with a .lnk extension. Symbolic links appear as a file or folder with a given name that may be different or the same as the target. The majority of applications would be oblivious to the fact that the file or folder they are accessing is really located somewhere else.

A [**hard link**](javascript://) can point only to a file on the same partition or volume as the hard link object. A hard link is a duplicate directory entry that points to the contents of a target file. When users or applications access a hard link, they believe the file content exists in the folder holding the hard link. Multiple hard links can point to the same target file. If the hard link’s target file is deleted from the target’s original location, the content can still be accessed through any hard link that still points to the content. The file’s content is preserved until the original file and all hard links that point to it are deleted.

A [**junction point**](javascript://) is a special type of symbolic link that points to folders only. The path to the target folder must be specified using an absolute path. The absolute path points to a target that can be located without needing to know the location of the original junction point object. Windows 10 makes frequent use of junction points to organize and optimize system data such as user profile folders, for example. Most end users are not aware of, or recognize the use of, junction points.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-8cResilient File System (ReFS)

[**Resilient File System (ReFS)**](javascript://) is a newer file system introduced with Windows Server 2012 that is included in Windows 10 but in a restricted capacity. It was originally envisioned as a candidate to replace NTFS as the default file system for persistent local storage. After many revisions, the capability to create ReFS volumes was removed from Window 10 v1709 (2017 Fall Creator’s Update) except for Enterprise and Pro for Workstation editions. All versions of Windows 10 retain the capability to read and write to existing ReFS disks. ReFS is not a general-purpose file system that is ready to replace NTFS.

The ReFS file system on a Windows 10 system is complementary to the resilient nature of storage spaces. ReFS is designed to verify and autocorrect data faults on the volume without having to bring the volume down for maintenance. Data integrity and correction testing is performed routinely as a background task to ensure that the file system has the highest level of uptime possible. This is considered practical for advanced Windows 10 configurations in an enterprise but not for the typical small/medium business or consumer configuration.

ReFS cannot be used to format the system boot volume, or on removable media. Some NTFS features are not included in the current ReFS file system in Windows 10, including some major features such as 8.3 file name support, file and folder compression, disk quotas, extended attributes, and [**Encrypting File System (EFS)**](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-8dUniversal Disk Format (UDF)

The Universal Disk Format (UDF) is a file system developed as a standard to allow file interchange between different operating systems. This makes it ideal for storing files on portable CD-ROM and DVD media. Windows 10 supports both reading and writing of files to the UDF file system.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-9**File System Tasks

After a partition or volume is formatted with a file system, few changes to the filesystem’s base configuration are possible. The most common file system changes are changing the assigned drive letter and converting the installed file system.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-9aChanging Drive Letters

Drive letters are used by applications and users as a quick reference to locate files. A drive letter points to a partition or volume formatted with a file system.

Once a drive letter has been used to reference a particular group of files, users and their applications expect the same drive letter to be used when the files are accessed again. This is especially true for a drive where Windows and apps are installed. Changing the drive letter for those drives can result in a broken system or apps that fail to run.

In some instances, the drive letter assigned to a partition or volume must change. For example, a new application might be installed that requires a specific drive letter to access data files, perhaps to mirror old settings hard-coded into an application. You can change the drive letter, or assign a new one, to a partition or volume by using the Disk Management console.

**Caution**

Some partitions, such as recovery and system partitions, should not be assigned a drive letter, as they are not meant to be accessed by users.

When a new partition or volume is created, one of the New Simple Volume wizard’s tasks asks if a drive letter should be assigned. Any unused drive letter can be selected. A single drive letter can be assigned to only one partition or volume.

Drive letters can also be removed from a partition or volume. If a drive letter is removed, the files might become inaccessible to the user.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-9bConverting File Systems

The only file system conversion that you can perform in Windows 10 that retains data is converting a volume from FAT/FAT32 to NTFS. You can use the convert command-line utility for this purpose. You can also change the file system for a volume when you reformat the volume, but all data on the volume is deleted during this process.

To convert a FAT file system to NTFS, perform these general steps:

1. Back up the data on the partition.
2. Ensure free space remains on the partition.
3. Convert the partition using the convert command-line utility.

**Caution**

Any file system conversion has a risk of failure, and, as a best practice, before you start you should have a backup available to recover the data or roll back the change.

The convert command-line utility has the syntax of convert drive\_id /FS:NTFS**.**

The drive\_id is the drive letter, mount point, or volume name used to identify which partition to convert. The command-line option /FS:NTFS tells the utility to convert the existing file system to NTFS.

For example, the command to convert drive N: to NTFS is:

* convert N: /FS:NTFS

Converting a partition requires that the convert utility runs with full administrative access to the local computer. If the file system is currently in use, the computer might have to reboot several times to complete the conversion process.

To retain data when you convert a ReFS or NTFS file system to FAT, perform the following general steps:

1. 1

Back up the data on the partition.

1. 2

Reformat the partition with FAT32.

1. 3

Restore the data originally backed up from the NTFS partition.

Go to pg.

[**help**](javascript://)

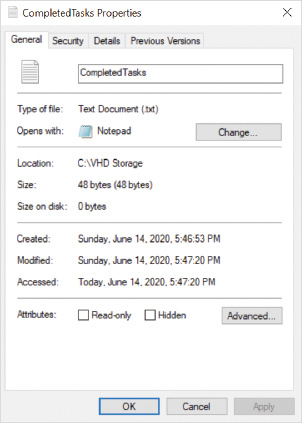
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-10**File and Folder Attributes

When you view the properties of a file or folder you can see a variety of useful information, as shown in [Figure 5-6](javascript://). The details reported for the properties of a file or folder change slightly depending on the type of item, file, or folder, and the file system (FAT, NTFS, or ReFS). For the most part, however, they have the same general information.

**Figure 5-6Properties of a File on an NTFS File System, General Tab**



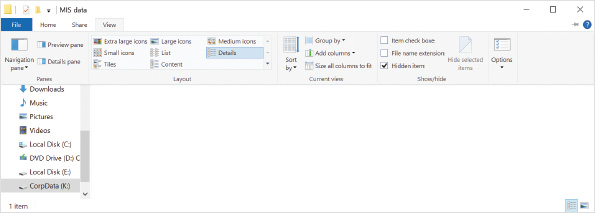
A few items worth noting in the properties of a file:

* The Size and Size on disk are not exactly the same. This is because disk space is allocated based on the cluster size you chose when you formatted the drive.
* Created, Modified, and Accessed time can all be useful when trying to identify the current version of file that users are working on.
* If you modify the application that a file type opens with, it is changed for all files with that file extension, not just the file you are modifying.

Each file or folder also has attributes. Attributes control how the operating system interacts with the file or folder. For example, when the read-only attribute for a file is turned on, the contents of the file can’t be modified. The General tab in the Properties of a file allows you to control the following attributes:

* Read-only—When a file is marked as read-only, the contents of the file can’t be modified. When you turn on the read-only attribute for a folder, it configures existing files in that folder and subfolders as read-only. New files created in the folder will not have the read-only attribute enabled.
* Hidden—The hidden attribute controls visibility of the file when using File Explorer or other utilities. Files with the hidden attribute enabled are not visible by default, but you can configure File Explorer to show hidden files, as shown in [Figure 5-7](javascript://).

**Figure 5-7File Explorer, View Tab, Option to Show Hidden Items**

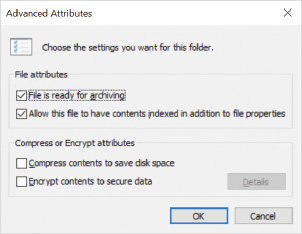


Enlarge Image

File Explorer also gives you access to advanced attributes. [Figure 5-8](javascript://) shows the advanced attributes available for a file on the NTFS file system. The advanced attributes are as follows:

* *File is ready for archiving*—The archive attribute is automatically enabled by Windows 10 when a file is modified. This attribute is used by backup software to identify files that should be backed up. You can manually enable or disable the archive attribute, but this is rarely required.
* *Allow this file to have contents indexed in addition to file properties*—You can disable this option to prevent the contents of a file from being indexed by Windows search. This affects search results returned by File Explorer.
* *Compress contents to save disk space*—When you enable the compress attribute on a file, a compression algorithm is applied by Windows 10 and storage space required by the file is reduced. When you enable the compress attribute on a folder, you get the option to compress existing files in that folder and all new files created in the folder have the compress attribute enabled by default.
* *Encrypt contents to secure data*—The encrypt attribute is used to secure file contents with Encrypting File System (EFS). By default, an EFS encrypted file is accessible only to the user that encrypts it, but access can be granted to additional users. When you enable the encrypt attribute on a folder, you get the option to encrypt existing files in that folder and all new files created in the folder have the encrypt attribute enabled by default.

**Figure 5-8Properties of a File on an NTFS File System, General Tab, Advanced Attributes**

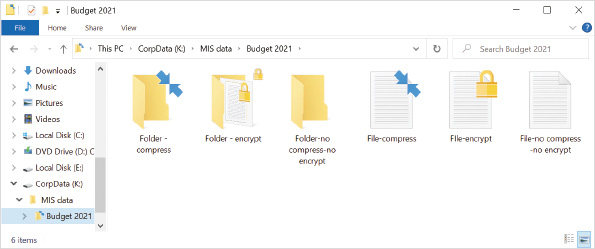


**Tip**

You can’t combine the compress and encrypt attributes.

To make it easier to identify compressed and encrypted files and folders, they are displayed with a unique icon in File Explorer, as shown in [Figure 5-9](javascript://). Compressed files and folder have two arrows pointing at each other. Encrypted files and folders have a lock symbol.

**Figure 5-9Modified Icons to Indicate Compressed Files and Folders in File Explorer**



Enlarge Image

**Note 11**

For more information about EFS, see [Module 6](javascript://) Windows 10 Security Features.

The system attribute is used by Windows 10 to identify files that should not be accessed or modify by users. When a file has the system and hidden attributes set, it is not displayed by File Explorer unless you disable the Hide protected operating system files (Recommended) folder option. You cannot modify the system attribute by using File Explorer.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-10aManaging Attributes

Most attribute flags can be viewed in File Explorer as part of the object’s properties. The **[attrib](javascript://)** command-line utility is used to manage the System and other advanced attributes, such as no scrub and integrity attribute flags, which cannot be accessed using File Explorer (advanced attributes, such as no scrub and integrity are relevant only with the ReFS file system when it is used with Storage Spaces; therefore, it’s not necessary to make those attributes generally available through File Explorer). The compression and encryption attribute flags cannot be managed by using the attrib command. Instead, the [**compact**](javascript://) command-line utility is used to manage the compress attribute flag, and the [**cipher**](javascript://) command-line utility is used to manage the encrypt attribute flag.

When you are at a command prompt and using the dir command, files or folders with the hidden attribute are not displayed by default. You can use dir to display files and folders with specific attributes set. For example, dir /as shows files and folders with the system attribute set.

In Windows PowerShell, the dir command is an alias for the Get-ChildItem cmdlet. The Get-ChildItem cmdlet does not show hidden files and folders by default. To view hidden files and folder, you need to use the -Force parameter, for example, Get-ChildItem -Force.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-10bCopying and Moving Compressed Files

When a file is copied, the original file is left in its old location, and a new file is created in the target folder. The newly created file always receives new attributes in the NTFS file system based on the attributes of the target folder. This means the compress attribute on the new file becomes the same as the target folder’s compress attribute setting. This is true whether the destination folder is in the same NTFS partition or another NTFS partition.

When a file is moved, the behavior of the compression attribute varies depending on whether the file is moved within the same partition or moved to a different partition. When a file is moved to a new location in the same NTFS partition, its attributes don’t change. This means the compress attribute on the file remains the same regardless of the target folder default setting.

When a file is moved from its current location to a new location in a different NTFS partition, new attributes are created in the destination’s NTFS system files. This means the compress attribute on the file becomes the same as the target folder’s compress attribute setting.

**Tip**

When a file is copied or moved to a destination folder that does not support compression (formatted with the FAT or ReFS file system, for example), the new copy of the file is uncompressed.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-11**File and Folder Permissions

Every file and folder stored on an NTFS or ReFS partition has its own [**access control list (ACL)**](javascript://). Each [**access control entry (ACE)**](javascript://) in the ACL identifies a specific user or group and what action they can perform to a file or folder. Each ACE uses a security identifier (SID) to identify the user or group, but the user interface for managing permissions displays the name of the user or group instead. Files and folders stored with other file systems such as FAT or FAT32 do not have an ACL. In the following section, note that NTFS permission settings apply equally to ReFS security.

NTFS permissions apply security to files and folders that impact any user trying to access the object. This applies equally to local users and network users. For example, if the ACL in a file system specifies deny access to a file, then access is denied regardless of how the file is being accessed.

**Note 12**

Refer to command-line parameters for the icacls utility by visiting [https://docs.microsoft.com/windows-server/administration/windows-commands/icacls](https://docs.microsoft.com/windows-server/administration/windows-commands/icacls" \t "_blank).

NTFS permissions are typically modified with File Explorer, but advanced changes can also be made from PowerShell using the cmdlets Get-ACL and Set-ACL, or the command-line utility **[icacls](javascript://)**. The icacls utility is very powerful but can be cryptic in its usage.

**Tip**

The icacls utility parameter */*reset can replace permissions with default inherited ACLs, which can be very useful if custom permissions are badly broken and need to be reset.

Windows 10 applies specific default permissions to folders when a partition is first formatted with the NTFS file system.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11aDefault Folder Permissions

The first level of folder in an NTFS partition is the root folder. The default permissions assigned to this folder on the C: drive are as follows:

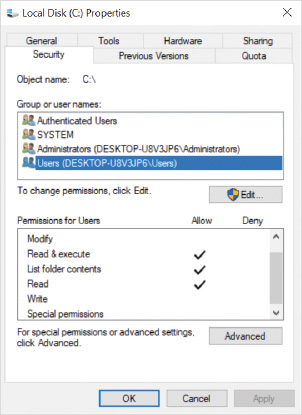
* Members of the computer’s Administrators group have full control.
* The operating system has full control.
* Members of the computer’s Users group have the ability to read and execute programs.
* Authenticated users have the ability to create folders in this folder.
* Authenticated users have the ability to create files and write data in subfolders only.

**Tip**

By default, users do not have the ability to create files in the root folder of the C: drive.

You can view the permission for a file or folder by using File Explorer. The Security tab in the Properties of the file or folder, shown in [Figure 5-10](javascript://), displays a summary of the permissions. Select a specific user or group to view the permissions assigned to that user or group.

**Figure 5-10Security Tab for an NTFS Drive’s Properties**



The default permissions assigned to subfolders on the C: drive, and the root folder on all other NTFS partitions are as follows:

* Members of the computer’s Administrators group have full control.
* The operating system has full control.
* Members of the computer’s Users group have the ability to read and execute programs.
* Authenticated users have the ability to create, modify, and delete files and folders in this folder and its subfolders.

As additional folders and files are created, they inherit permissions from the parent object that contains them. Inheritance allows a permission setting to be configured at a higher level in the file system and have it propagate to lower subfolders and files.

**Note 13**

Basic NTFS permissions were called standard NTFS permissions in previous versions of Windows. Likewise, advanced NTFS permissions were called individual NTFS permissions in previous versions of Windows.

NTFS permissions are assigned using the following two formats:

* Basic NTFS permissions
* Advanced NTFS permissions

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11bBasic NTFS Permissions

Basic NTFS permissions represent a collection of predetermined advanced NTFS permissions. The combination of advanced permissions provides a general level of access specific to the type of basic permission assigned. For example, the basic NTFS permission of Modify is a collection of advanced NTFS permissions that allows a file to be read, written to, renamed, or deleted. The names of basic NTFS permissions are meant to be intuitive and easy to understand. The basic NTFS permissions are listed in [Table 5-4](javascript://).

**Table 5-4**

### Basic NTFS Permissions

| **Permission** | **Description** |
| --- | --- |
| Write | This permission used for folders allows new files and folders to be created in the current folder. The folder attributes can be changed and the folder’s ownership and security can be viewed.  This permission used for files allows file data to be rewritten. The file’s attributes can be changed and the file’s ownership and security can be viewed. |
| Read | This permission used for folders allows files and folder data, attributes, ownership, and security to be viewed. This permission used for files allows the file’s data, attributes, ownership, and security to be viewed. |
| List folder contents | This permission applies only to folders. Without this permission, the files and folders contained in a folder cannot be listed. The user or application can still access the files if they have permission and know the exact file or folder name. |
| Read & execute | This permission used for folders allows read access to files and folders below this point. This is the equivalent of enabling Read and List folder contents.  This permission used for files allows read access to the file’s information and, if it is an executable file, the user is allowed to run it. This permission automatically includes the Read permission. |
| Modify | This permission used for folders allows the same actions as Write and Read & execute permissions combined. The folder can also be deleted.  This permission used for files allows the same actions as Write and Read & Execute permissions combined. Files can also be deleted. |
| Full Control | This permission used for folders allows the same actions as Modify plus the ability to change permissions and allow a user to take ownership of the folder.  This permission used for files allows the same actions as Modify plus the ability to change permissions and allow a user to take ownership of the file. |
| Special permissions | Special permissions are the advanced permissions that can be assigned when the predefined basic permissions are not adequate to achieve desired results. |

Enlarge Table

Go to pg.

[**help**](javascript://)

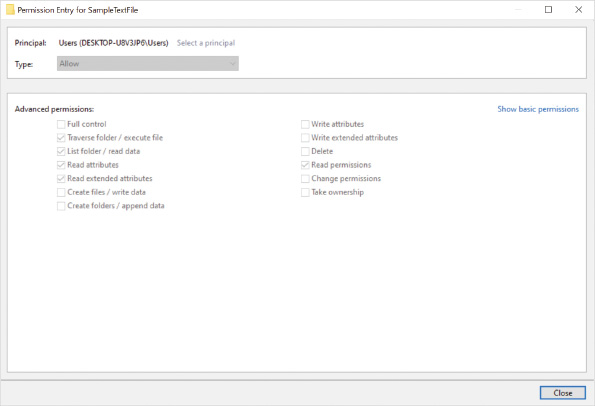
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11cAdvanced NTFS Permissions

Many advanced NTFS permissions exist to fine-tune access and control for files and folders. The list of advanced permissions is visible only when editing a permission entry in the Advanced security view, shown in [Figure 5-11](javascript://).

**Figure 5-11Viewing Advanced NTFS Permissions on a File for One ACL Entry**



Enlarge Image

It is much more complex to configure advanced NTFS permissions because the name and purpose of the individual advanced permissions are often not intuitive. It is a best practice to use basic NTFS permissions wherever possible. This avoids complex special security settings that are unnecessarily difficult to manage.

Go to pg.

[**help**](javascript://)

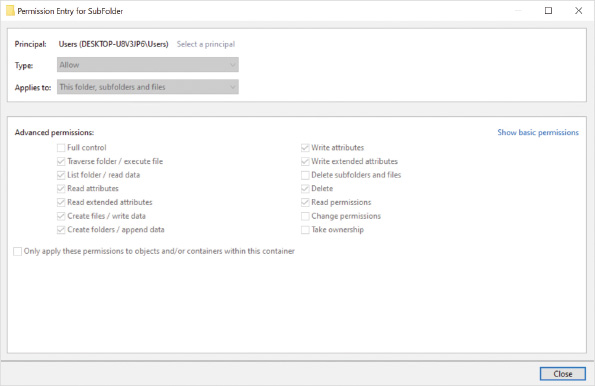
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11dPermission Scope

When an NTFS permission setting is applied to a file or folder, it also has a scope assigned. The scope determines what other objects are impacted by the assigned permission. For files, the scope is limited to this object only, which is just the file itself. For folders, you can configure the scope in the Applies to box of the advanced security view, as shown in [Figure 5-12](javascript://). When you configure basic NTFS permissions on a folder the scope is automatically configured as This folder, subfolders and files.

**Figure 5-12Viewing Advanced NTFS Permissions on a Folder for One ACL Entry**



Enlarge Image

For folders, the scope can be set to:

* This folder only
* This folder, subfolders, and files
* This folder and subfolders
* This folder and files
* Subfolders and files only
* Subfolders only
* Files only

**Caution**

Consider the permission scope carefully to ensure that you obtain the desired inheritance effect.

Go to pg.

[**help**](javascript://)

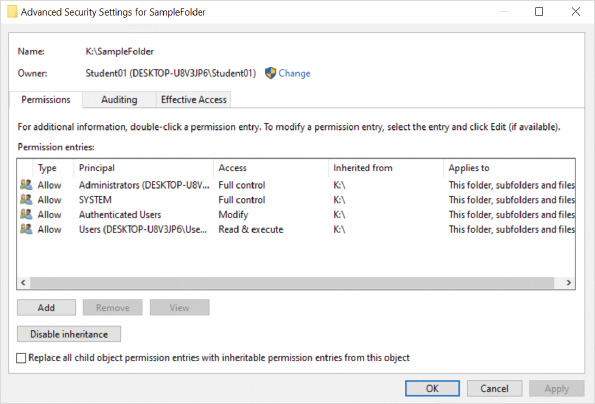
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11ePermission Inheritance

NTFS permissions are inherited to files and subfolders based on the permission scope defined on the parent folder. Typically, permissions propagate from a parent folder to all files and folders below that point. When viewing the Permissions tab in advanced security settings for a folder, the Inherited from column shows where a permission setting was first applied, as shown in [Figure 5-13](javascript://). Further changes to those permission assignments automatically propagate through folders and files below that point. Any files created in those folders inherit permissions from the folder in which they are located.

**Figure 5-13Advanced Security Settings for an NTFS Folder**



Enlarge Image

Inheritance of permissions is convenient, but it might not be desired for all situations. Each file or folder has a Disable inheritance option in the Advanced Security Settings dialog box to disable inheritance of that object.

Disabling inheritance blocks inheritance of permissions from higher levels of the file system. Once inheritance is disabled, a prompt appears asking if the old inherited permissions should be copied to the object or removed entirely so that you can start with new permissions. If the previous permissions are copied, they provide a starting point and can be customized to meet any requirements. If the permissions are removed, new permissions must be configured from scratch.

Any file or folder can have additional permissions assigned directly to the object that combine with the inherited permissions. This combination of inheritance and explicit permissions at any level allows for flexibility, but you must be very careful that the combination of permissions gives you the desired security result.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11fEffective Permissions

Effective permissions are the combination of permissions assigned to the user and permissions assigned to groups that the user is a member of. You need to add the user and group permissions to determine the effective permissions. If a user is assigned read permission and a group the user is a member of is assigned write permission, then the effective permissions for the user are read and write.

**Tip**

Permissions assigned to groups are easier to manage and audit than assigning permissions directly to users. The user’s group membership is much easier to manage than remembering all the places that need to be updated in the file system’s permissions.

Effective permissions include permissions directly assigned to the file and folder, as well as inherited permissions. If permissions are assigned directly to a file for a specific user, then those permissions override any inherited permissions that were assigned for that user. For example, if a user is assigned full control permissions to a folder and the user is also assigned read permission directly to a file inside that folder, then the effective permission is Read, because it is changing the user specific permission. If some of the permissions are assigned to a group and some permissions are assigned to the user, then they’re not overridden. For example, if the Users group is assigned full control permissions to a folder and the user is assigned read permission directly to a file inside that folder, then the effective permission is full control.

You also need to consider that permissions can allow permissions or deny permissions. When some permissions are allow and other permissions are deny, you need to understand the order of precedence:

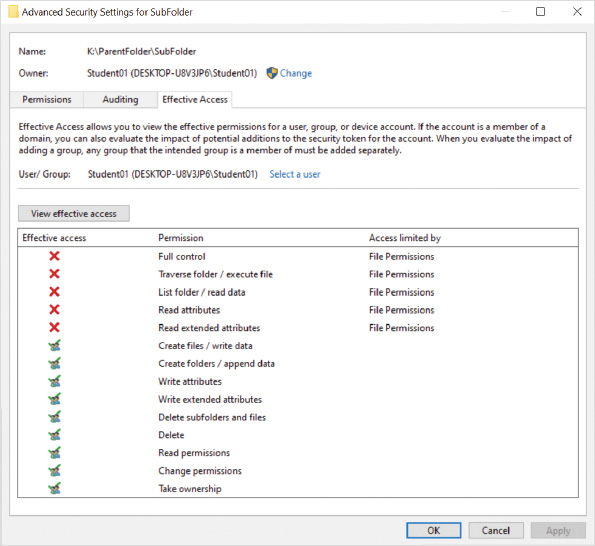
1. Explicit deny
2. Explicit allow
3. Inherited deny
4. Inherited allow

Some other considerations for permissions are as follows:

* Each permission has a scope that determines what range of objects to which it applies.
* Users that do not have explicit permission assigned to an object and are not part of any inherited permission have no permission to the object.
* Users can be members in multiple groups that have different permissions to the same object.
* Owners of a file or folder have full control of the object.

To simplify the analysis of effective permissions, the Advanced Security Settings window for any file or folder includes an Effective Access tab, as shown in [Figure 5-14](javascript://). When you select a user or group on the Effective Access tab, the advanced NTFS permissions which are effective for that group or user are displayed. This tool doesn’t show how those effective permissions were obtained; it shows only what they are. You still need to review permissions on folders above to identify how the permissions were obtained.

**Figure 5-14Effective Access Tab in Advanced File or Folder Security Settings**



Enlarge Image

**Caution**

The Effective Access tab in a file or folder’s Advanced Security Settings does not include ownership as part of its effective permission calculations.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11gOwnership

Each NTFS file or folder has an owner assigned to it. The owner of a file or folder always has the ability to assign permissions to that file or folder, regardless of which existing permissions are assigned. This ensures that the owner can always assign himself Full control permission and modify a file.

Members of the Administrators group have the right, by default, to assign or take ownership of a file or folder. Users with the Full control basic permission or the advanced NTFS permission Take ownership can also assume ownership of a file.

You can view or modify the owner of a file or folder in the Advanced Security Settings window when using File Explorer. At a command prompt, you can use the icacls or **[takeown](javascript://)** utilities to configure ownership. In Windows PowerShell, you can use the Get-Acl and Set-Acl cmdlets to view and modify ownership.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11hPermission Changes When Content Is Copied or Moved

When files and folders are first created in a volume that is formatted with NTFS, they take on the permission settings of the folder in which they are created. Copy operations always create new versions of the content that is being copied. Those new versions take on the permission settings of the target location, which might be different than the permission settings of the source content. Move operations affect permissions differently depending on the destination location relative to the source location.

Each single volume or partition formatted with the NTFS file system has its own database to track permissions and attributes for each file and folder it stores. When files and folders are moved from one location on the volume to another location on the same volume, new content is not created; only pointers to the content are moved in the database. In that case, the destination content keeps whatever permissions it originally had, regardless of the destination folder’s permissions.

When files and folders are moved from one volume to a different volume formatted with NTFS, new content is created in the destination location. Just like a copy operation, the new content takes on the permission settings of the target location. Any permission settings assigned to the source content are lost.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-11iPermission Strategy Considerations

Assigning and managing file permissions is seldom required for computers running Windows 10. Administrators have full access to the entire file system as required for any maintenance. Users have full access to their own profiles to store documents and application data. Users do not have access to the profiles of other users or the ability to modify system files. In the vast majority of scenarios, this is what you want.

In rare cases, an application might require you to modify the file system permissions to run properly. For example, some applications that use a nonstandard update process require you to give users modify permission to the application folder. Then, the user is able to run the script that copies files and updates the application.

Most of the detailed considerations about applying file and folder permissions are more relevant for configuring permissions on a shared folder on a server. On a server, you might have a shared folder with multiple folders inside it. Each of the folders in the shared folder might have different permissions for different departments.

**Activity 5-9:**

### Managing File and Folder Permissions

**Time Required:**30 minutes

**Objective:**Configure a new folder with unique NTFS security settings

**Description:**In this activity, you create a new folder called Marketing Documents on the C: drive. The default permissions are removed and replaced with permissions that allow only your user account to access the folder. You then create a file in the folder and investigate its resulting inherited permissions.

1. 1

You should already be signed in from the previous activity.

1. 2

Right-click the **Start** button and then click **File Explorer**.

1. 3

In the left pane, click **Local Disk (C:)**.

1. 4

Create a new folder called **Marketing Documents** in C:\.

1. 5

Right-click the **Marketing Documents** folder and then click **Properties**.

1. 6

In the Marketing Documents Properties dialog box, click the **Security** tab and review the users and groups assigned permissions.

1. 7

Click the **Advanced** button and review the specific permissions that have been applied to the users and groups.

1. 8

In the Advanced Security Settings for Marketing Documents dialog box, click the **Effective Access** tab.

1. 9

Click the **Select a user link** to display the Select User or Group dialog box.

1. 10

Type your user name and then click **OK** to continue.

1. 11

Click the **View effective access** button. On the Effective Access tab, notice which advanced NTFS permissions have a check mark next to them. You have all available permissions because your account is a local administrator.

1. 12

Note the current owner of the folder. Your account is the owner of the folder because you created it. Click the **Change** link to the right of the name in the Owner field.

1. 13

In the Select User or Group dialog box, type **Administrators** and then click **OK** to change the owner of the folder to the local Administrators group and any user that belongs to that group.

1. 14

Select the **Replace owner on subcontainers and objects** check box.

1. 15

If necessary, click the **Change Permissions** button to enable the controls for changing permissions.

1. 16

Click the **Disable inheritance** button.

1. 17

In the Block Inheritance warning dialog box, click **Remove all inherited permissions from this object** to start with blank security settings for the Marketing Documents folder.

1. 18

Click the **Add** button in the Advanced Security dialog box to display the **Permission Entry** dialog box.

1. 19

Click **Select a principal** link.

1. 20

Enter your user name and then click **OK** to continue.

1. 21

In the list of basic permissions, place a check next to the **Full control** permission.

1. 22

Note that all other basic permissions are automatically assigned and that the permission scope is set to **This folder, subfolder and files**.

1. 23

Click **OK** to continue.

1. 24

Note the new permission entry on the Permissions tab in the Advanced Security Settings dialog box.

1. 25

Notice that the Inherited from column shows as None for the directly assigned permission.

1. 26

Click **OK** to close the Advanced Security Settings dialog box.

1. 27

Click **OK** to close the Marketing Documents Properties dialog box. This is required to refresh the contents of that window.

1. 28

Right-click the **Marketing Documents** folder and then click **Properties**.

1. 29

Click to select the **Security** tab. Notice the new permission setting and the simpler view.

1. 30

Click **OK** to close the Marketing Documents Properties dialog box.

1. 31

Create a new text document called **First Quarter Report.txt** in the **C:\Marketing Documents** folder.

1. 32

Right-click **First Quarter Report.txt**, click **Properties**, and then click the **Security** tab. Notice that the permissions from the Marketing Documents folder are inherited by this file, as indicated by the grey check marks.

1. 33

Click **Cancel** and close all windows and dialog boxes.

1. 34

To release all open and attached VHDs, plus the active storage pool created with virtual disks, restart your computer. These virtual disks will not reattach automatically the next time you sign in.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**5-12**File Sharing

Windows 10 provides multiple ways to share files from one computer to another. The best method for sharing files will depend on the scenario. For example, the Share tab in File Explorer is a simple interface for sharing individual files, but shared folders are a better mechanism for keeping many files in a central location.

**Caution**

Early versions of Windows 10 included the HomeGroup feature to simplify file sharing in a home or workgroup environment. This feature was removed in Windows 10 version 1803, but you might still find documentation that references it.

Go to pg.

[**help**](javascript://)

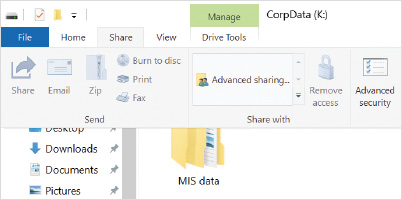
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-12aSharing Individual Files

The Share tab in File Explorer, shown in [Figure 5-15](javascript://), is designed for users with basic needs, users who are not trying to fine-tune or tweak shared item security. It simply enables the users to get what they want—the selected file(s) sent to somewhere or someone else. This method of file sharing sends a copy of the file to the recipient. If you update the source file, the recipient won’t get the updated version unless you send it again.

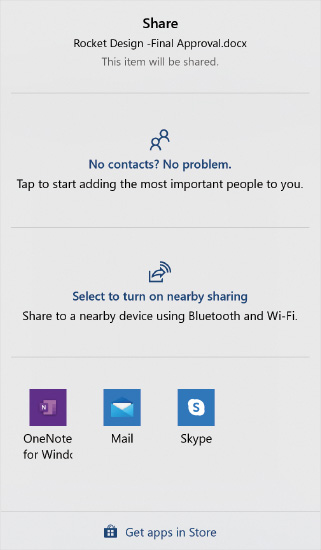
**Figure 5-15Share Tab in File Explorer**



After selecting the files you want to share, click the Share button to select a sharing method. It will open a window, as shown in [Figure 5-16](javascript://), where:

* The recipient can be selected from the signed in user’s contact list and a copy is sent via email.
* The content is shared through Bluetooth or Wi-Fi. For this feature to work, nearby sharing must be enabled in Setting’s Shared experiences, as shown in [Figure 5-17](javascript://).
* Files can be shared via an app, such as OneNote, Mail, or Skype. Additional apps like Dropbox can be added to the list of Apps by visiting the Microsoft Store.

**Figure 5-16File Explorer, Share Tab, Send Group, Share Option, Possible Recipients**



Enlarge Image

**Figure 5-17Settings App, System, Shared Experiences**



Enlarge Image

You can also access these file sharing options by right-clicking a local file in File Explorer and then clicking Share on the shortcut menu. This is a convenience for quickly sharing files—if you right-click a local folder you will not see that option.

**Caution**

If you right-click a file in a folder that is synchronized with OneDrive, you may see a cloud symbol next to the word Share on the shortcut menu. Selecting this opens a window to craft a custom link that you can send to someone, which they will use to access the shared content in that user’s OneDrive. This is not the same Share experience mentioned earlier for local files, and the link can be used with folders and files.

Go to pg.

[**help**](javascript://)

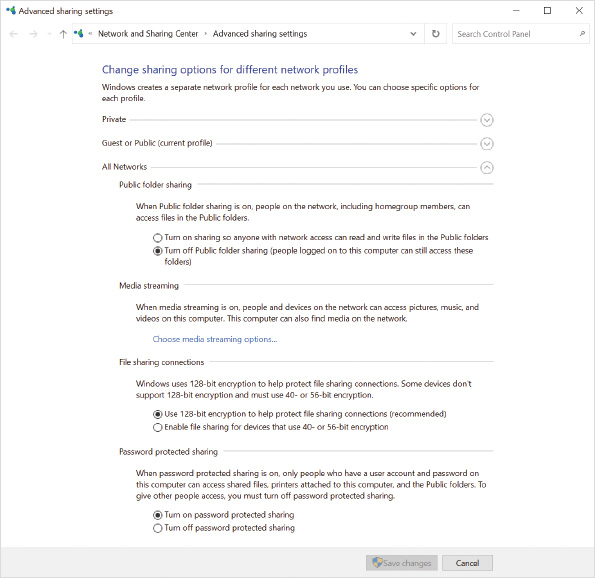
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-12bSharing the Public Folder

The Public folder is typically located at C:\Users\Public. Sharing the Public folder is a simplified way to perform file sharing on home and small office networks. By default, all files in the Public folder are shared among users who sign in sitting at the same local computer, giving those users a way to share data locally. The Public folder, however, can also be shared with network users. Sharing for the Public folder is configured by using the Public folder sharing option in Advanced sharing settings in the Network and Sharing Center, as shown in [Figure 5-18](javascript://).

**Figure 5-18Public Folder Sharing Controls**



Enlarge Image

The options for sharing the Public folder are as follows:

* Turn on sharing so that anyone with network access can read and write files in the Public folders—When this option is selected, all network users are able to read, change, delete, and create files in the Public folder. A Public folder configured this way could be used as a central storage location for business documents in a small business to ensure that files can be easily found and are able to be backed up each night.
* Turn off Public folder sharing (people signed in on this computer can still access these folders)—When this option is selected, only local users (i.e., those sitting at the computer) can access files in the Public folder.

You also have options for Password protected sharing that also apply to the Public folder, also shown in [Figure 5-18](javascript://). Password protection offers two options. These options also apply to other shared folders and printers.

* Turn on password protected sharing—When this option is selected, network users must sign in to the sharing computer by using a user account that has been granted access to the sharing computer. The account can be either a local user account or a domain user account. This allows you to restrict access to the shared Public folder to valid user accounts, but you cannot select which user accounts have access. All valid user accounts are able to access the shared Public folder.
* Turn off password protected sharing—When this option is selected, anyone can access the information in the Public folder, even if they do not have a valid user account on the sharing computer. Effectively, this allows anonymous users access to the Public folder.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-12cCreating and Managing Shared Folders

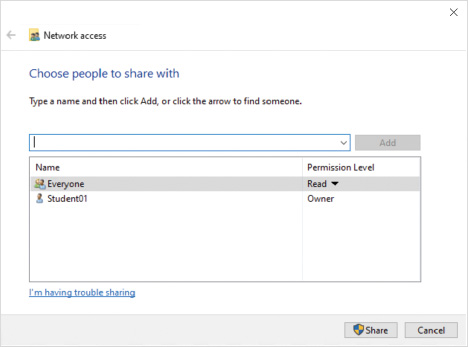
Sharing files from specific folders on your computer gives you more options to manage which users have access to those files and what those users can do to those files. You can set the permissions for users when you share individual folders. For example, in a small business, the users in your project team may be given permission to view and change your shared project files, but your other coworkers are able only to view the files.

The ability to configure shared folder permissions may be confusing for inexperienced users, but for experienced users the level of control allows you to configure file sharing just the way you want it. In a domain-based network, you can select users from the domain to share files with. In a workgroup-based network, you must create local accounts for the users you want to share files with. For example, if you want to share files with Bob, who signs in to another computer, you must create a user account for Bob on your Windows 10 computer, and then give the local user Bob permission to access files.

### Simplified Folder Sharing

Simplified folder sharing provides a limited set of security options to configure shared folders. The folder sharing wizard, shown in [Figure 5-19](javascript://), manages the shared folder settings and NTFS permissions based on the options that you select. This hides the details behind a user-friendly interface that is suitable for end users without complex needs.

**Figure 5-19Folder Sharing Wizard**



The folder sharing wizard contains an arrow that you can use to select the users or groups to which you want to assign permissions. By default, only the Everyone group and local user accounts are displayed in the list. If you want to add other users or groups, you need to type the user or group name instead of selecting from the list. The following permission levels are shown in the folder sharing wizard:

* Owner—This identifies the user that is the owner of the folder. You can’t assign which user is the owner; this permission is just displayed.
* Read/Write—This permission grants users the Full Control NTFS permission.
* Read—This permission grants users the Read & Execute NTFS permission.

**Caution**

The NTFS permissions configured by the folder sharing wizard remove any existing NTFS permissions in the folder being shared and any subfolders.

After the folder sharing wizard creates the share, it displays the [**Universal Naming Convention (UNC) path**](javascript://) for the shared folder. The UNC path includes the name of the Windows 10 computer and the name of the share. For example, \\Desktop48\Data. You need to give this UNC path to other users so that they know where to access the shared folder over the network.

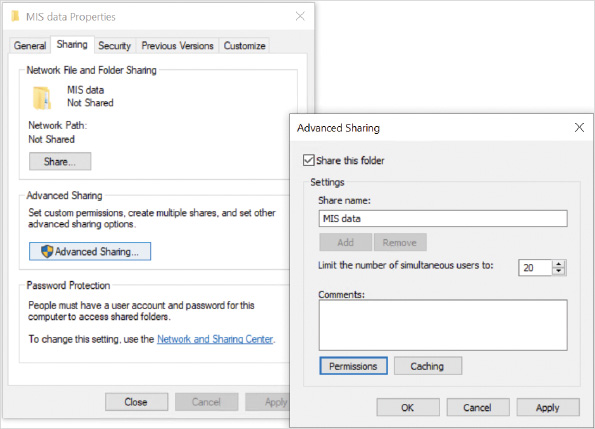
The folder sharing wizard can be triggered in multiple ways:

* Use the Share button on the Share tab in the Properties of a folder.
* Right-click a folder, point to Give access to, and select Specific people.
* Select Specific people in the Share with area on the Share tab in File Explorer.

### Advanced Folder Sharing

Advanced folder sharing allows you precise control over the permissions assigned to the shared folder and the NTFS permissions in the file system. The interface for advanced folder sharing allows you to configure only the share permissions. You need to configure the NTFS permissions as a separate task. You access advanced folder sharing by clicking the Advanced Sharing button on the Sharing tab in the Properties dialog box of a folder, as shown in [Figure 5-20](javascript://).

**Figure 5-20Folder Properties, Advanced Sharing**



Enlarge Image

Following are the settings you can configure in Advanced Sharing:

* Share this folder—This option enables the folder as shared.
* Share name—This option allows you to specify one or more names that the folder is shared as. By default, the share name matches the folder name. Users access the shared folder by using the UNC path \\computername\sharename. Each additional share name is associated with its own set of shared folder permissions and limits on concurrent users. For example, if the folder has two share names, it is accessible using two different UNC paths. The UNC path a user uses to access the shared folder will determine which shared folder permission and limits apply to that shared folder connection over the network.

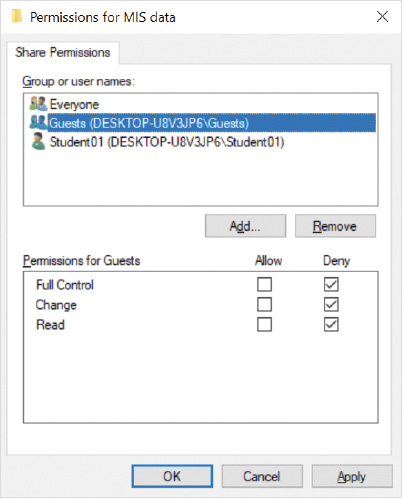
**Tip**

Share names ending in a dollar sign ($) are hidden shares that cannot be seen by browsing the network. You can use the dollar sign at the end of your own shared folder names so that the folder will be accessible only if the user knows the appropriate UNC path to use. This is not considered a strong security mechanism alone, as there are numerous ways to discover these so-called hidden shares.

* Limit the number of simultaneous users to—Windows 10 supports up to 20 concurrent connections from network users. With this setting, you can reduce this to a lower number to ensure that the computer is not overwhelmed by network users; however, this is typically not done because sharing files has very little effect on performance.
* Comments—This box contains text that is displayed for users when they view the share on the network. Typically, the text describes the content in the shared folder.
* Permissions—This button lets you configure the share permissions for the shared folder.
* Caching—This button lets you control how network clients cache files from this share as offline files. You can prevent file caching, allow users to select files for caching, or force file caching. Caching files for offline use is typically done only for mobile computers.

When you configure share permissions, the permissions can be allow or deny permissions, as shown in [Figure 5-21](javascript://). When a permission is denied, it overrides any permissions that are allowed. For example, if the Everyone group is given Read permission and the user Bob is denied Read permission, Bob will not have access to the share.

**Figure 5-21Folder Properties, Advanced Sharing, Permissions**



The share permissions available in Windows 10 are the following:

* Full Control—Allows users complete control over files and folders in the share and sets permissions on files and folders in the share. In addition, Full Control allows users to configure the share permissions on the shared folder.
* Change—Allows users complete control to create, modify, and delete files in the shared folder, but not to set permissions.
* Read—Allows users to read the contents of files in the shared folder, but not to modify the files in any way.

If the local file system does not support additional security, for example the FAT file system, the shared folder permissions are the only security settings that apply when that folder is accessed from the network. The Security tab won’t even show up on the folder’s properties, only the Sharing tab. That’s why most administrators prefer the custom security provided by combining shared folder permissions with local NTFS file and folder permissions.

Some special considerations should be taken when shared folder permissions combine with NTFS permissions—the most restrictive permissions are effective when the file is accessed over the network. If the user is sitting at the keyboard and signing in locally (i.e., interactively), only the NTFS file and folder permissions apply.

For example, if a user is assigned Read share permissions and Full control NTFS permissions, the user will have only read access when accessing the folder over the network. If a user is assigned Full Control share permissions and Read NTFS permissions, the user will also have only read access when accessing the folder over the network. Both of these permission combinations result in the same effective permission for accessing files in the folder over the network—read; however, consider that when the user signs in directly to that computer, the user’s permission to the folder and its contents are different in each case.

To simplify the management of permissions, you can assign the Full Control share permission to the Everyone group and then use NTFS permissions to apply more restrictive access to the folders and files in the shared folder. This has the added benefit of ensuring that user permissions are the same for accessing folders and files whether a user accesses the content over the network or by signing in to the local computer.

**Tip**

When you use simplified folder sharing, Full Control share permissions are assigned and NTFS permissions are used to control access.

### Create A Shared Folder Wizard

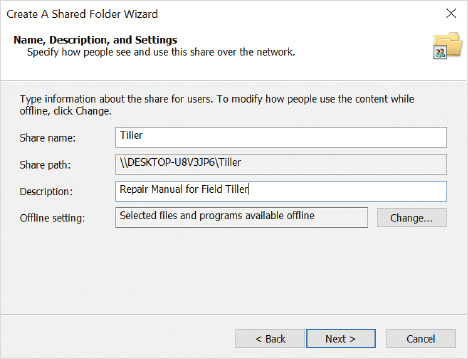
Computer Management includes the capability to create, manage, and monitor shared folders. When you create a shared folder from within Computer Management, it triggers the Create A Shared Folder Wizard.

**Tip**

The Create A Shared Folder Wizard can also be running the shrpubw.exe utility.

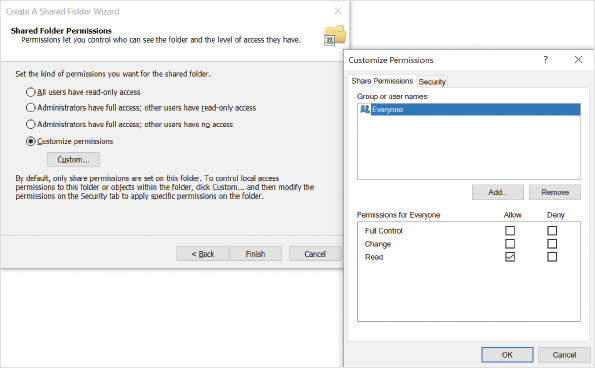
You can select an existing local folder or create a new folder on the computer with this wizard. Once a folder is selected, the options to configure for the share, shown in [Figure 5-22](javascript://), are similar to the advanced sharing wizard’s configuration options.

**Figure 5-22Create A Shared Folder Wizard, Specify Folder Settings**



The Create A Shared Folder Wizard will ask if you want to configure one of the more common shared folder permission combinations or enable you to configure custom permissions that conveniently include shared folder permissions and NTFS file permissions, as shown in [Figure 5-23](javascript://).

**Figure 5-23Create A Shared Folder Wizard, Shared Folder Permissions**



Enlarge Image

**Caution**

This wizard can be used to create multiple shares for the same local folder, but you do not manage existing shared folder settings from here—you must use the advanced sharing button from the shared folder’s properties.

### PowerShell for Sharing Folders

You can use Windows PowerShell cmdlets to create and manage shared folders. It is more common to use graphical tools, but if you need to automate the creation of shared folder on multiple computers, then using the cmdlets can be useful. The cmdlets include Smb because Windows 10 file sharing is based on the [**Server Message Block (SMB)**](javascript://) protocol. The primary cmdlets for managing shared folders are listed in [Table 5-5](javascript://).

**Table 5-5**

### PowerShell Cmdlets for Managing Shared Folders

| **PowerShell Cmdlet** | **Description** |
| --- | --- |
| Get-SmbShare | Retrieves the properties of the SMB shares on the computer. |
| Get-SmbShareAccess | Retrieves the share permissions of the SMB share. |
| Grant-SmbShareAccess | Adds or modifies share permissions for a user or group. |
| New-SmbShare | Creates an SMB share. |
| Remove-SmbShare | Deletes the specified SMB share. |
| Revoke-SmbShareAccess | Removes the share permissions for a user or group. |
| Set-SmbShare | Modifies the properties of the SMB share. |

### Net Commands to Share Folders

The [**net command-line utility**](javascript://) is a legacy tool that can be used to perform a wide variety of tasks, such as creating users and creating shared folders. You might see this utility used in older scripts that were created many years ago but are still in use. Examples of net commands to manage shared folders are listed in [Table 5-6](javascript://).

**Table 5-6**

### Net Command Examples for Managing Shared Folders

| **Example Net Commands** | **Description** |
| --- | --- |
| Net Share DataFolder=C:\workfiles | Shares the folder C:\workfiles as a shared folder called DataFolder, with default permission that everyone has read access to the shared folder. |
| Net Share DataFolder=C:\workfiles /grant:everyone,full | Shares the folder C:\workfiles as a shared folder called DataFolder but grants the Everyone built-in group full access permission to the shared folder. |
| Net Share DataFolder /delete | Stops sharing the shared folder called DataFolder. |

**Caution**

The net command-line tool still works with Windows 10; however, it has been deprecated since Windows 8.

**Activity 5-10**

### Creating Shared Folders

**Time Required:**15 minutes

**Objective:**Create shared folders for network users

**Description:**Multiple methods are available to create shared folders. To ensure that shared folders meet your needs, you need to understand the differences among the methods for creating shared folders. In this activity, you create shared folders using multiple methods.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **File Explorer**. In the left pane, click to select the **Documents** location.

1. 3

Right-click the empty area in the right pane, point to **New**, and then click **Folder**.

1. 4

Type **SimpleShare1** and then press **Enter**.

1. 5

Click **SimpleShare1** and then click the **Share** menu on the toolbar.

1. 6

Select **Specific people** in the Share with area on the toolbar. Click the arrow in the box next to the Add button, click **Everyone**, and then click the **Add** button. Notice that the default permission given to Everyone is Read.

1. 7

To the right of Everyone, click **Read** and then click to select **Read/Write**. This allows Everyone to modify files.

1. 8

Click the **Share** button.

1. 9

If you are prompted to turn on network discovery and file sharing for all public networks, click **Yes, turn on network discovery and file sharing for all public networks**. This is a suitable choice for a lab environment, but this would likely not be a good idea if the computer were going to be used in an untrusted environment, such as an Internet café.

1. 10

Read the results in the File Sharing window. Notice that the UNC path for this share is long and goes through the C:\Users folder. All folders shared by using simple file sharing in your Documents folder use this long UNC path.

1. 11

Click **Done**.

1. 12

In the File Explorer window currently displaying the Documents library, double-click **Local Disk (C:)** below Computer in the left pane.

1. 13

Right-click an open area in the right-hand pane, point to **New**, and then click **Folder**.

1. 14

Type **SimpleShare2** and then press **Enter**.

1. 15

Right-click an open area, point to **New**, and then click **Folder**.

1. 16

Type **AdvancedShare** and then press **Enter**.

1. 17

Right-click **SimpleShare2**, point to **Give access to**, and then click **Specific people**.

1. 18

On the Choose people to share with screen, click the arrow, click **Everyone** in the list, and then click the **Add** button.

1. 19

To the right of Everyone, click **Read** and then click **Read/Write**.

1. 20

Click the **Share** button.

1. 21

On the Your folder is shared screen, read the results and notice that the UNC path is directly to the shared folder when the folder is not inside your Documents folder.

1. 22

Click **Done**.

1. 23

Right-click the **AdvancedShare** folder and then click **Properties**.

1. 24

Click the **Sharing** tab and then click **Advanced Sharing**.

1. 25

Select the **Share this folder** check box. Notice that the Share name setting is the same name as the folder by default, but it can be changed.

1. 26

Click the **Permissions** button to view the share permissions.

1. 27

Select the **Allow** check box next to the **Change** permission and then click **OK**. This allows all users to modify files through the share, but not to change the share permissions.

1. 28

Click **OK** to close the Advanced Sharing dialog box.

1. 29

Click the **Security** tab and then click the **Edit** button.

1. 30

Click **Add**, type **Everyone**, click **Check Names**, and then click **OK**.

1. 31

In the Group or user names box, click **Everyone** to select the built-in group.

1. 32

In the Permissions for Everyone box, select the **Allow** option next to the **Modify** permission and then click **OK**. NTFS permissions work with the share permissions to control what tasks a user is able to perform on a network share. These steps have configured the Everyone group and its members to have the same permission to the folder when accessed over the network, and locally at the keyboard, granting read/write access to its contents.

1. 33

Click **Close** to close the AdvancedShare Properties dialog box.

1. 34

Close all open windows and/or dialog boxes.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 5-12dMonitoring Shared Folders

Over time, you might lose track of all the folders that are shared on your computer. You can use PowerShell cmdlets, net commands, and the Computer Management console to review what is shared and who is connecting to it.

### PowerShell to Monitor Shared Folders

The primary PowerShell cmdlets for managing SMB-based shares are listed in [Table 5-7](javascript://). Using PowerShell cmdlets for folder monitoring requires administrative rights to the computer.

**Table 5-7**

### PowerShell Cmdlets for Monitoring Shared Folders

| **PowerShell Cmdlet** | **Description** |
| --- | --- |
| Get-SmbConnection | Retrieves the connections established from the SMB client to an SMB server. |
| Get-SmbOpenFile | Retrieves basic information about the files that are open on behalf of the clients of the SMB server. |
| Get-SmbSession | Retrieves information about the sessions that are currently established between the SMB server and the associated clients. |
| Get-SmbShare | Retrieves the SMB shares on the computer. |
| Get-SmbShareAccess | Retrieves the Access Control List of the SMB share. |

### Net Commands to Monitor Shared Folders

Viewing shared folder details from the command prompt can be accomplished with the legacy net command, even without administrative rights to the computer. Examples of net commands to monitor shared folders are listed in [Table 5-8](javascript://).

**Table 5-8**

### Net Command Examples for Monitoring Shared Folders

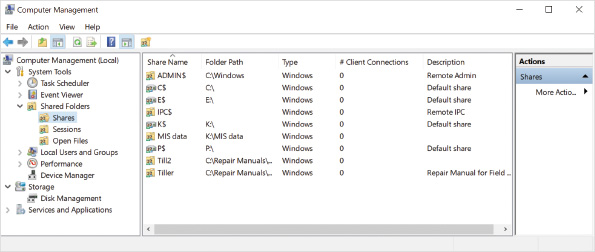
| **Example Net Commands** | **Description** |
| --- | --- |
| Net Session | Displays information about all sessions with the local computer, including computer names, user names, number of files open, and session idle time. |
| Net Share | Displays information about all the resources that are shared on the local computer. |
| Net view \\localhost | Displays a list of resources that are being shared by the specified computer. |
| Net view \\localhost /ALL | Displays a list of resources that are being shared by the specified computer, including the hidden shares with $ at the end of their name. |

### Computer Management to Monitor Shared Folders

The most comprehensive way to monitor shares is by using Computer Management, shown in [Figure 5-24](javascript://). The Shared Folders system tool has the following three nodes for monitoring and managing shared folders:

* Shares—This node allows you to create new shares, configure existing shared folders, and optionally stop sharing them. It shows all of the shared folders on this computer, including hidden shares. The summary view here even allows you to see how many clients are connected to each share.
* Sessions—This node allows you to see which users are connected to this computer. The summary view shows which computer each user is connecting from, how many files each user has open, and how long each user has been connected. If your system has the maximum of 20 sessions already connected and you need to allow another user access, you can disconnect an existing session from here.
* Open Files—This node allows you to see which files and folders are opened through file shares on this computer. You can see which users have the files open and whether the file is open for writing. Occasionally, due to system problems, users will be disconnected from files, but Windows 10 keeps the file locked. You can force a file to close here so that it can be reopened and modified.

**Figure 5-24Shares View in Computer Management**



Enlarge Image

**Activity 5-11**

### Monitoring Shared Folders

**Time Required:**5 minutes

**Objective:**Monitor shared folders by using Computer Management

**Description:**When you share folders on your computer, it is useful to see who is using those files. For example, if you want to reboot your computer, you must be sure that no files are open. Rebooting a computer with shared files open can corrupt the files. In this activity, you monitor shared folders on your computer.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Computer Management**.

1. 3

In the left pane, expand **Shared Folders** and then click **Shares**. This displays all the shares on your computer, including the hidden shares. You can see the Users, SimpleShare2, and AdvancedShare shares from previous activities. You can also see the number of clients connected to each share and the folder each is sharing.

1. 4

Right-click **SimpleShare2** and then click **Properties**. The General tab allows you to configure the name of the share, description, user limit, and offline settings.

1. 5

Click the **Share Permissions** tab and then, if necessary, click **Everyone**. This tab allows you to configure the share permissions for the share. Notice that the Everyone group has Full Control.

1. 6

Click the **Security** tab, and in the Group or user names box, if necessary, click **Everyone**. This tab displays the NTFS permissions for the folder. Notice that Everyone has Full Control NTFS permissions. These NTFS permissions were automatically configured by the Grant access to simple sharing wizard in the previous activity.

1. 7

Click **Cancel** to close the SimpleShare2 Properties dialog box.

1. 8

In the left pane of the Computer Management window, click **Sessions**. The Sessions folder shows you which users are connected to your computer and from which computer they are connected.

1. 9

In the left pane of Computer Management, click **Open Files**. The Open Files folder shows you which files and folders are open on your computer and by which user.

1. 10

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 5-13a**Summary**

* Windows 10 supports internal, external, virtual, and pooled disks (dynamic and Storage Spaces).
* Windows 10 supports MBR and GPT partition styles to organize data into partitions and volumes on physical and virtual disks.
* Disk management tools include the Disk Management Tools, Diskpart, and storage cmdlets in Windows PowerShell.
* When you add a new physical disk to a computer, you might need to adjust firmware settings or scan for new drives. You also need to initialize the new disk to define the partition style for the disk. When you move a physical disk to a new computer, initialization is not required.
* VHDs are natively supported by Windows 10 and can be managed as a basic disk once the VHD is attached in the operating system. VHD files can either be a fixed size or allowed to grow dynamically to a maximum size. You need to attach a VHD in Windows to view and modify the contents.
* Storage Spaces technology is software based and is used to combine physical disk drives into a managed storage pool, which is then used to create virtual volumes from that combined space. Depending on the number of physical disks in the pool, Storage Spaces volumes can be created with a selected resiliency level.
* The NTFS file system is preferred in Windows 10 because it supports advanced features, such as security, ownership, disk quotas, compression, and encryption that FAT does not. Small partitions can still benefit from the legacy support and simplicity of FAT. ReFS has a subset of NTFS features but does not support disk quotas, compression, or encryption.
* When you format a partition or volume, you select a drive letter and a file system. It is possible to change the drive letter afterwards if required. You can also convert use the convert utility to change the file system from FAT to NFTS without data loss.
* Files stored in FAT, ReFS, and NTFS partitions use attributes to control and limit file access. Some attributes are: read-only, hidden, archive, compress, and encrypt.
* Given an NTFS-formatted source location, a copy operation will create content in a destination location. A move operation will only create content in a destination location when the destination is in a different NTFS volume. Newly created content will take on the permissions of the destination folder in which they were created.
* NTFS and ReFS share a security model that is configured by assigning permissions to users or groups. Basic permissions are suitable for most scenarios, but advanced permissions can be used for more specific control if required. To properly calculate effective permissions, make sure that you understand permission scope and inheritance.
* File sharing allows you to share files and folders on one computer with another user on a different computer. The Share button in File Explorer allows you to send individual files. Simplified and advanced folder sharing make a folder and its contents available over the network. Advanced folder sharing allows you to configure share permissions and NTFS permissions separately.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 5-13b**Key Terms**

* [**access control entry (ACE)**](javascript://)
* [**access control list (ACL)**](javascript://)
* [**attrib**](javascript://)
* [**basic disk**](javascript://)
* [**cipher**](javascript://)
* [**compact**](javascript://)
* [**Disk Management console**](javascript://)
* [**disk quotas**](javascript://)
* [**DiskPart**](javascript://)
* [**dynamic disks**](javascript://)
* [**Encrypting File System (EFS)**](javascript://)
* [**File Allocation Table (FAT)**](javascript://)
* [**Foreign Disk**](javascript://)
* [**fsutil**](javascript://)
* [**GUID Partition Table (GPT)**](javascript://)
* [**hard link**](javascript://)
* [**icacls**](javascript://)
* [**initialize**](javascript://)
* [**junction point**](javascript://)
* [**Master Boot Record (MBR)**](javascript://)
* [**MBR2GPT**](javascript://)
* [**mklink**](javascript://)
* [**net command-line utility**](javascript://)
* [**New Technology File System (NTFS)**](javascript://)
* [**partition table**](javascript://)
* [**Resilient File System (ReFS)**](javascript://)
* [**Server Message Block (SMB)**](javascript://)
* [**storage pool**](javascript://)
* [**Storage Spaces**](javascript://)
* [**Storage Spaces volume**](javascript://)
* [**symbolic link**](javascript://)
* [**takeown**](javascript://)
* [**Universal Naming Convention (UNC) path**](javascript://)
* [**virtual hard disk (VHD)**](javascript://)
* [**volume mount points**](javascript://)
* [**volumes**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 5-13c**Review Questions**

1. A user has been given Full Control permission to a shared folder. The user has been given Modify permission at the NTFS level to that folder and its contents. What is that user’s effective permissions to that folder when they access it through the shared folder from another computer?
   1. Full Control
   2. Modify
   3. Read
   4. No access
2. Which sharing method should you recommend if a user wants to configure share and NTFS permissions for another user that wants to access a folder on their computer in a single simple process?
   1. Public folder sharing
   2. Grant access to
   3. advanced sharing
   4. Create A Shared Folder Wizard
3. Which sharing method does not allow you to pick the folder that is being shared?
   1. Public folder sharing
   2. simple sharing
   3. advanced sharing
   4. Create A Shared Folder Wizard
4. What is the most accurate way to view all the shares on your system?
   1. Browse your computer on the network.
   2. View the shares in Computer Management.
   3. Use the Show me all the shared network folders on this computer link.
   4. Use the Show me all the files and folders I am sharing link.
   5. View the shares in the Network and Sharing Center.
5. Which type of startup firmware best supports Windows 10 with regard to device operation and management?
   1. BIOS
   2. GPT
   3. UEFI
   4. MBR
6. A VHD has been created using the Disk Management utility. Before the newly created VHD can be used to store files, it must be .
   1. detached
   2. configured as a dynamic disk
   3. set to GPT partition style
   4. initialized
   5. set to MBR partition style
7. A storage  acts as a logical container grouping multiple physical disks.
8. You have just plugged a USB portable hard drive into an older laptop and the disk has not appeared as available. You are concerned that the hard disk controller hardware has not been recognized by the computer. Which utility would you use to verify that the controller is functioning correctly?
   1. DiskPart
   2. Disk Management console
   3. USB Management console
   4. Device Manager
   5. none of the above
9. The number of physical disks required to implement three-way resilience for a Storage Spaces volume is .
   1. 1
   2. 2
   3. 3
   4. 5
   5. 7
10. The preferred technology to set up disk storage with mirrored fault tolerance for a user’s backup data is
    1. basic disks
    2. dynamic disks
    3. hardware-based RAID 5
    4. Storage Spaces
    5. hardware-based RAID 1
11. An NTFS partition has disk quotas enabled. You would like to run a weekly report that summarizes how much space each user is consuming. The  utility allows you to review quota details from the command line.
    1. convert
    2. fsutil
    3. get-diskquota
    4. diskpart
    5. dsquota
12. Windows 10 supports locally encrypted files stored on these types of partitions (Select all that apply).
    1. NTFS
    2. ReFS
    3. FAT
    4. FAT32
13. The  file system is the only one that supports file compression in Windows 10.
    1. FAT32
    2. ReFS
    3. NTFS
    4. FAT
14. A file is currently compressed in its local file system. For security reasons, the file is required to be encrypted. The file can be both compressed and encrypted. True or False?

True

False

1. A user is given Read permission to a file stored on an NTFS-formatted volume. The file is then moved to a different folder on a different NTFS-formatted volume where the user has been given Modify permission for that folder. The file is then moved to a folder on a FAT32-formatted volume. When the user signs in to the computer holding the file and accesses it via a drive letter, what is the user’s effective permission to the file?
   1. Read
   2. Change
   3. Full control
   4. Modify
   5. It will lose its permissions
2. A user is assigned Read permission to the NTFS folder C:\ACCOUNTING as required by company policy. The user requires full access to the subfolder C:\ACCOUNTING\FORMS and its contents. This can be best accomplished by .
   1. not possible
   2. blocking permission inheritance at C:\ACCOUNTING\FORMS and assigning the user ownership of C:\ACCOUNTING\FORMS
   3. assigning the user Full control to C:\ACCOUNTING
   4. blocking permission inheritance at C:\ACCOUNTING and assigning the user Full control to C:\ACCOUNTING\FORMS
   5. assigning the user Full control to C:\ACCOUNTING\FORMS
3. A user checks the free space in a folder on their local computer, Y:\BusReports, and notices that 3 GB of disk space is reported as available. When the user checks free space in Y:\BusReports\Archive, he notices that 50 GB of disk space is reported as available. The difference in available disk space is probably because the folder Y:\BusReports\Archive is .
   1. archived
   2. compressed
   3. encrypted
   4. dynamic
   5. a mount point
4. Upon opening the Disk Management console, you notice a disk whose status is reported as Foreign Disk. This is most likely because .
   1. the disk must be initialized
   2. the disk has been corrupted
   3. the disk is shared on the network
   4. the disk was moved from another computer
5. A user is given Read permission to a file stored on an NTFS-formatted volume. The file is then moved to a different folder on a different NTFS-formatted volume where the user has been given Full control permission to that folder. When the user signs in to the computer holding the file and accesses its new location via a drive letter, what is the user’s effective permission to the file?
   1. Read
   2. Full control
   3. No access
   4. Modify
   5. none of the above
6. A user is given Read permission to a file stored on an NTFS-formatted volume. The file is then moved to a folder on the same NTFS-formatted volume, where the user has been given Modify permission to that folder. When the user signs in to the computer holding the file and accesses its new location via a drive letter, what is the user’s effective permission to the file?
   1. Read
   2. Full control
   3. No access
   4. Modify
   5. none of the above

Go to pg.

[**help**](javascript://)