MICROSOFT
TRAINING
AND CERTIFICATION

Microsoft Official
Curriculum

Module 13: Configuring and Managing File Systems

Contents

Microsoft®

Instructor Notes

Presentation:
60 Minutes

Labs:
45 Minutes

This module provides students with the knowledge and skills necessary to configure and manage file systems on computers running Microsoft® Windows® XP Professional.

After completing this module, the student will be able to:

- Describe the differences between the various files systems supported by Windows XP Professional.
- Compress data on an NTFS file system volume.
- Copy and move compressed files.
- Encrypt and decrypt data on an NTFS volume.

Materials and Preparation

This section provides the materials and preparation tasks that you need to teach this module.

Required Materials

To teach this module, you need Microsoft PowerPoint® file 2272A_13.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussions.
- Anticipate student questions about material and write out answers to those questions.

Instructor Setup for a Lab

This section provides setup instructions that are required to prepare the instructor computer or classroom configuration for a lab.

Lab 13A: Configuring Disk Compression

► **To prepare for the lab**

1. The lab requires that the student computers are running Windows XP Professional.
2. Drive C on the student computers must be configured with the NTFS file system.

Lab 13B: Securing Files by Using EFS

► **To prepare for the lab**

1. The lab in this module requires that the student computers are running Windows XP Professional.
2. Drive C on the student computers must be formatted with the NTFS file system.
3. The student lab files encrypt1.txt and encrypt2.txt must be installed on the student computers. The student lab files are located in C:\MOC\2272\Labfiles\mod13.

Module Strategy

Use the following strategy to present this module:

- Working with File Systems

  This section provides an overview of the various types of file systems supported by Windows XP Professional. Focus on the factors to consider when selecting a file system, including volume and cluster size, compatibility with operating systems, and file system capabilities. Point out that NTFS is the preferred file system with Windows XP Professional. Distinguish between formatting and conversion and discuss how to convert FAT and FAT32 volumes to NTFS. Discuss compatibility of NTFS volumes on Windows XP Professional with NTFS volumes on Microsoft Windows 2000 and Microsoft Windows NT®.

- Managing Data Compression

  This section introduces NTFS data compression. Begin by describing the benefits of compression and explaining that compression occurs at either the file or folder level. Pointing out that a compressed folder can contain uncompressed files and compressed files can reside in an uncompressed folder. Describe what occurs when a file or folder is compressed and demonstrate how to compress a file. Demonstrate how to change the color of compressed files in Windows Explorer. Describe the effect of moving and copying compressed files within a volume and between volumes. Conclude this section by discussing best practices for managing NTFS compression.

- Lab A: Configuring Disk Compression

  In this lab, students configure an NTFS volume for compression. Students then experiment moving and copying files and folders to both compressed and uncompressed folders. The lab enables students to view the effects that moving and copying files and folders have on compression states.

- Securing Data by Using EFS

  This section provides an overview of the Encrypting File System (EFS). Begin by describing the benefits of encryption. Describe the key features of EFS. Stress that encryption and decryption are local operation and cannot be used for network security. Describe the process of encryption demonstrating how to encrypt a file or folder, and how to add authorized users once the file is encrypted. Next, describe the process of decryption. Explain what occurs when backing up encrypted files. Then provide an overview of the function of a designated recovery agent. Review which user accounts that are default recovery agents. Conclude this section by reviewing best practices for implementing EFS.

- Lab B: Securing Files by Using EFS

  In this lab, students encrypt a folder and its contents. Next, they log off and log on to the computer by using a different user ID to verify that encryption was implemented, and view what occurs when an unauthorized user attempts to gain access to an encrypted file. Students then log off and log on to the computer by using their original Administrator logon, and decrypt the folder so that its contents will be accessible to all users.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Training and Certification courseware.

Lab Setup

The following list describes the setup requirements for the labs in this module.

- The labs in this module require that the computers are running Windows XP Professional.
- Complete Module 1, "Installing Microsoft Windows XP Professional," in Course 2272A, *Implementing and Supporting Microsoft Windows XP Professional (Course Beta).*

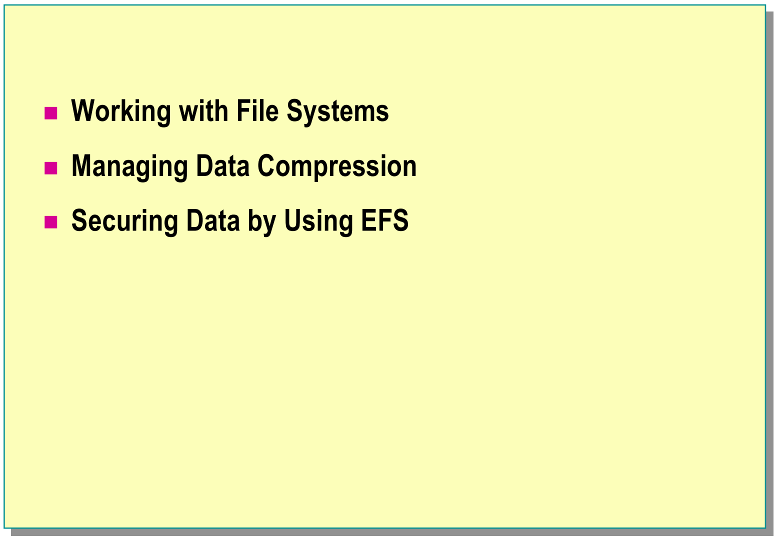
Lab Results

Performing the labs will result in no configuration changes to the student or instructor computers.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about the various file systems supported by Windows XP Professional and how to better manage the storage and security of those files.



- **Working with File Systems**
- **Managing Data Compression**
- **Securing Data by Using EFS**

A *file system* is the structure in which files are named, stored, and organized. Microsoft® Windows® XP Professional supports three types of file systems on hard disks:

- FAT (file allocation table)
- FAT32
- NTFS file system

It is important that you understand how file systems work so that you can select the file system or file systems that are best suited for your environment and tasks. You should also know how to manage files and folders and secure confidential and private files.

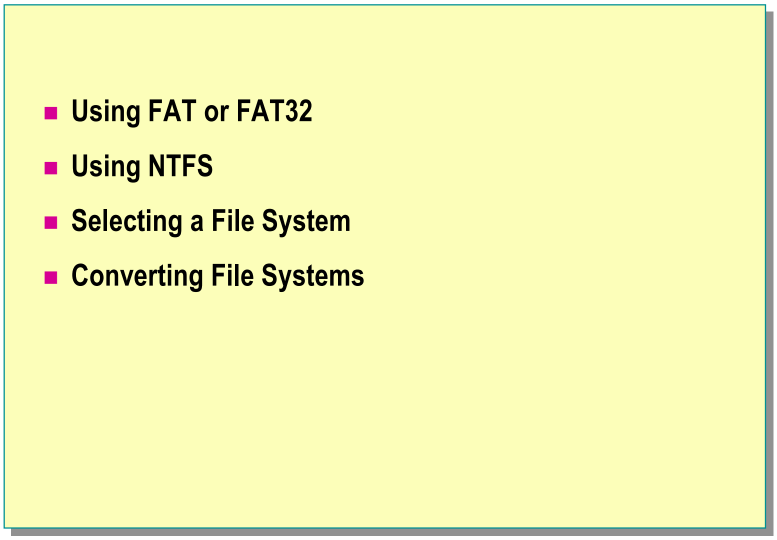
After completing this module, you will be able to:

- Describe the differences between the various files systems that are supported by Windows XP Professional.
- Compress data on an NTFS volume.
- Copy and move compressed files.
- Encrypt and decrypt data on an NTFS volume.

# ◆ Working with File Systems

Topic Objective
To introduce file systems that are available in Windows XP Professional.

Lead-in
There are several factors to consider when selecting a file system.



- Using FAT or FAT32
- Using NTFS
- Selecting a File System
- Converting File Systems

When choosing a FAT, FAT32, or NTFS file system, you must consider the features and functions that are associated with that file system. You must also consider limitations, such as maximum volume size, cluster size, file size, and compatibility with other operating systems.

Note The term volume is used in this module to refer to both basic volumes (that is, partitions on a basic disk) and dynamic volumes.

For Windows XP Professional, NTFS is the preferred file system. NTFS supports valuable functionality such as file compression, a higher level of security, and formatting of very large volume sizes for compatibility with the latest disk technology.

Key Points
NTFS is the preferred file system for Windows XP Professional.

Once you have converted a volume to NTFS, you cannot convert back to FAT or FAT32.

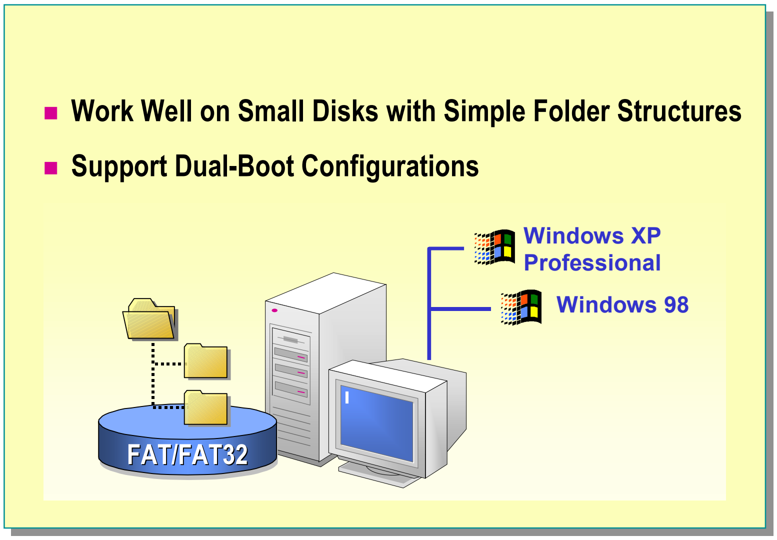
You can easily convert volumes from FAT or FAT 32 to NTFS when upgrading to Windows XP Professional. All data on existing FAT or FAT32 volumes is written to new NTFS volumes. You can also convert a volume to NTFS when adding a new disk or creating new volumes in Windows XP Professional.

Once you have converted a volume to NTFS, you cannot convert back to FAT or FAT32 without reformatting the volume.

Using FAT or FAT32

Topic Objective
To provide an overview of FAT and FAT32 capabilities.

Lead-in
Windows XP Professional supports FAT and FAT32 file systems. FAT or FAT32 are required if you are supporting a dual-boot configuration with previous versions of Windows that do not support NTFS.



- **Work Well on Small Disks with Simple Folder Structures**
- **Support Dual-Boot Configurations**

FAT is the file system that is used by Microsoft MS-DOS® and subsequent versions of Windows. FAT32 was introduced with Microsoft Windows 95 OSR2. Windows XP Professional supports both FAT and FAT32.

The major differences between FAT and FAT32 fall into three major categories:

- Volume size
- Cluster size
- Supported operating systems

FAT works best on small disks with simple folder structures. FAT32 works well on larger disks with more complex folder structures. The following table compares FAT with FAT32.

FAT	FAT32
Supports volume sizes up to 2 gigabytes (GB).	Supports volume sizes up to 32 GB. Volume can theoretically be as large as 2 terabytes, but Windows XP Professional limits the volume that you can format to 32 GB.
You must divide a large disk into volumes where no volume exceeds 2GB.	Greater flexibility on how you organize large disks: from many small volumes up to a single large volume not exceeding 32 GB.
Supports cluster sizes up to 64 KB for large volumes.	Supports smaller cluster sizes not exceeding 16 KB. Small cluster sizes are preferable because they reduce wasted space on hard disks.
Supports dual-boot configurations.	Supports dual-boot configurations.

Note Windows XP Professional can read and write to larger FAT32 volumes formatted by Microsoft Windows 98 and Microsoft Windows 2000.

Operating systems can only access the volumes that are formatted with a file system that the operating system supports. The following table shows the files systems that are supported on various Windows operating systems:

Operating System	Supports NTFS	Supports FAT32	Supports FAT
Windows XP Professional	Yes	Yes	Yes
Windows 2000 Professional	Yes	Yes	Yes
Microsoft Windows NT® version 4.0 Workstation	Yes	No	Yes
Windows 95 OSR2, Windows 98, and Microsoft Windows Millennium Edition	No	Yes	Yes
Windows 95 (prior to version OSR2)	No	No	Yes
MS-DOS	No	No	Yes

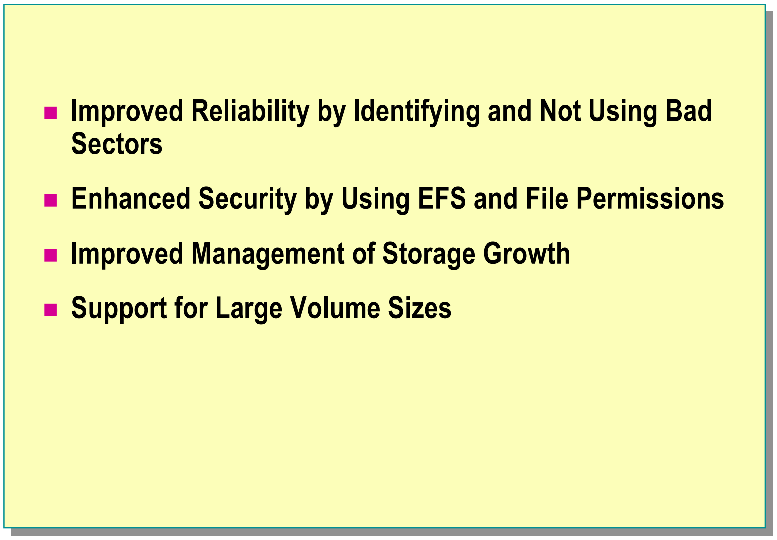
If you need a dual boot system, you must consider the operating systems that you are running when selecting a file system. Using Windows XP Professional with certain dual boot configurations may require you to use FAT or FAT32. The operating systems that would not require you to use FAT or FAT32 in a dual boot configuration are: Windows XP Professional, Windows 2000 Professional, and Windows NT 4.0 with Service Pack 4 or later.

Note Windows NT 4.0 with Service Pack 3 or earlier supports a version of NTFS that is not compatible with NTFS running on Windows XP Professional. If you require a dual boot system with these two operating systems, you would need to use FAT or FAT32 for Windows NT.

Using NTFS

Topic Objective
To provide an overview of NTFS capabilities.

Lead-in
NTFS is the preferred file system for Windows XP Professional because it enables file compression, provides a higher level of security, and supports formatting of large volumes.



- **Improved Reliability by Identifying and Not Using Bad Sectors**
- **Enhanced Security by Using EFS and File Permissions**
- **Improved Management of Storage Growth**
- **Support for Large Volume Sizes**

NTFS is a file system that is available on Windows NT, Windows 2000, and Windows XP Professional. It is not available on other versions of Windows operating systems. NTFS provides performance and features that are not found in either FAT or FAT32. NTFS provides:

- Reliability

  NTFS uses log file and checkpoint information to restore the consistency of the file system when the computer is restarted. In the event of a bad-sector error, NTFS dynamically remaps the cluster containing the bad sector and allocates a new cluster for the data. NTFS also marks the cluster as bad and no longer uses it.

- Greater security

  NTFS files use Encrypting File System (EFS) to secure files and folders. If enabled, files and folders can be encrypted for use by single or multiple users. The benefits of encryption are data confidentiality and data integrity, which can protect data against malicious or accidental modification. NTFS also enables you to set access permissions on a file or folder. Permissions can be set to Read Only, Read and Write, or No Access.

- Improved management of storage growth

  NTFS supports the use of disk quotas. Disk quotas enable you to specify the amount of disk space that is available to a user. By enabling disk quotas, you can track and control disk space usage. You can configure whether users are allowed to exceed their limits, and you can also configure Windows XP Professional to log an event when a user exceeds a specified warning level or quota limit.

  With NTFS you can easily create extra disk space by compressing files, extending volumes, or mounting a drive. File compression is discussed later in this module. For additional information on extending volumes and mounting drives, see Module 12, “Managing Disks,” in Course 2272A, *Implementing and Supporting Microsoft Windows XP Professional (Course Beta).*

- Support for larger volume sizes

  By using NTFS, theoretically you can format a volume up to 32 exabytes. NTFS also supports larger files and a larger number of files per volume than FAT or FAT32. NTFS also manages disk space efficiently by using smaller cluster sizes. For example, a 30-GB NTFS volume uses 4-KB clusters. The same volume formatted by using FAT32 uses 16-KB clusters. Using smaller clusters reduces wasted space on hard disks.

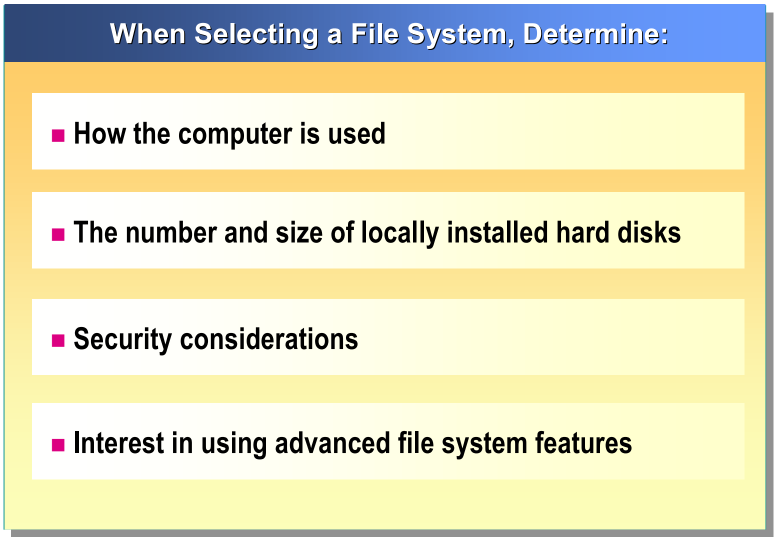
When NTFS was introduced with Windows NT, users continued to format system and boot volumes with FAT. In the event of a start-up failure, an MS-DOS bootable floppy disk could be used to help troubleshoot the problem. However, with Windows XP Professional, you no longer need to use FAT for the system and boot volumes because Windows XP Professional offers two troubleshooting tools that are designed to gain access to NTFS volumes:

- *Safe mode*. In this mode, Windows XP Professional starts by loading only the basic set of device drivers and system services.
- *Recovery Console*. This is a special command-line environment that enables you to copy system files from the operating system compact disc (CD), fix disk errors, and otherwise troubleshoot system problems without installing a second copy of the operating system.

Selecting a File System

Topic Objective
To discuss the factors that you should consider when selecting a file system.

Lead-in
You can use different file systems on a hard disk, but each volume can only be formatted with a single file system.



When Selecting a File System, Determine:

- How the computer is used
- The number and size of locally installed hard disks
- Security considerations
- Interest in using advanced file system features

You can use any combination of FAT, FAT32 or NTFS when formatting a hard disk, but each volume on a hard disk must be formatted by using only one of these file systems.

Key Points
You can use any combination of FAT, FAT32 or NTFS when formatting a hard disk, but each volume on a hard disk must be formatted by using only one file system.

When choosing the appropriate file system to use, you need to determine:

- If the computer has a single operating system or is a multiple-boot system.

  On computers that contain multiple operating systems, file system compatibility can be complex because different versions of Windows support different combinations of file systems.

- The number and size of locally installed hard disks.

  Each file system has a different maximum volume size. As volume sizes increase, your choice of file systems becomes limited. For example, both FAT 32 and NTFS can read volumes larger than 32GB, however only NTFS can be used for format volumes larger than 32 GB in Windows XP Professional.

- Security considerations.

  NTFS offers security features, such as encryption and file and folder permissions. These features are not available on FAT or FAT32 volumes.

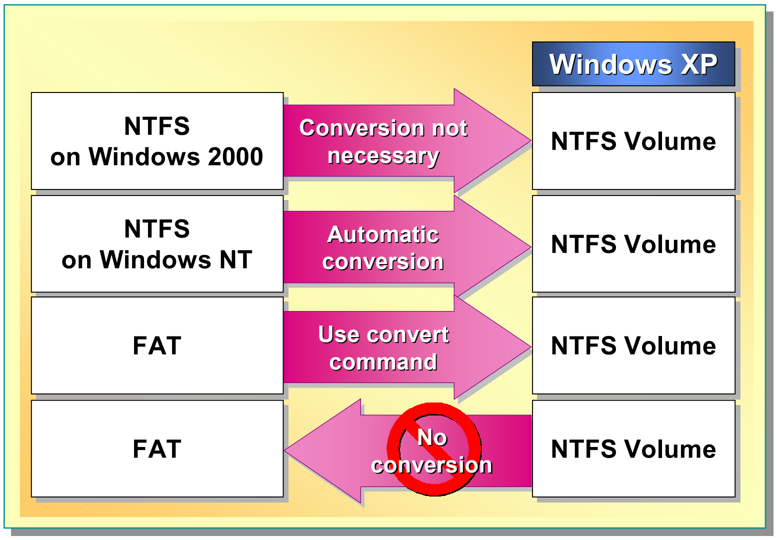
- Interest in using advanced file system features.

  NTFS offers features such as disk quotas, distributed link tracking, compression, and mounted drives. These features are not available on FAT or FAT32 volumes.

Converting File Systems

Topic Objective
To discuss conversion of files systems to NTFS on Windows XP Professional.

Lead-in
NTFS is supported on some but not all previous versions of Windows. Ability to convert to NTFS depends on both the existing file system and the operating system.



Converting a volume's file system is different from formatting a volume. You format a volume that has no previous file system format. You convert a volume's file system when changing the existing file format to a new file format. Windows XP Professional can convert FAT, FAT32, and NTFS in Windows NT to the version of NTFS in Windows XP.

Key Points
NTFS volumes for Windows XP Professional and Windows 2000 are the same.

NTFS volumes that are created by using Windows NT will upgrade automatically the first time that the volumes are accessed in Windows XP Professional.

You cannot convert NTFS volumes back to FAT volumes.

Using NTFS with Windows 2000 and Windows XP Professional

Windows 2000 and Windows XP Professional use the same version of NTFS. Therefore, no conversion occurs when Windows XP Professional first accesses an NTFS volume that was formatted by using Windows 2000.

Using NTFS with Windows NT 4.0 and Windows XP Professional

When you upgrade from Windows NT 4.0 to Windows XP Professional, all NTFS volumes that were formatted by using Windows NT 4.0 are upgraded to the new version of NTFS. The upgrade occurs when Windows XP Professional accesses the volume for the first time after Windows XP Professional Setup is completed. Any NTFS volumes that are removed or turned off during Setup, or added after Setup, are converted when Windows XP Professional accesses the volumes.

Converting FAT or FAT32 Volumes to NTFS

You can convert a FAT or FAT32 volume to NTFS by using the Setup program when upgrading to Windows XP Professional. If you choose to convert after you have installed Windows XP Professional, you can use Disk Management or the convert command from the command prompt window.

To use the convert utility to convert a volume to NTFS, at the command prompt, type:

```
convert drive letter: /FS:NTFS
```

Before you convert a FAT or FAT32 volume to NTFS, you must consider the following:

- Despite a minimal chance of corruption or data loss during the conversion from FAT to NTFS, it is recommended that you perform a full backup of the data on the volume to be converted before you convert to NTFS. It is also recommended that you verify the integrity of the backup before proceeding.
- The conversion is a one-way process. After you convert a volume to NTFS, you cannot reconvert the volume to FAT without backing up data on the NTFS volume, reformatting the volume as FAT, and then restoring the data onto the newly formatted FAT volume.
- Converting the file system requires a certain amount of free space on the volume and sufficient memory to update the cache. Ensure that you have sufficient available disk space.

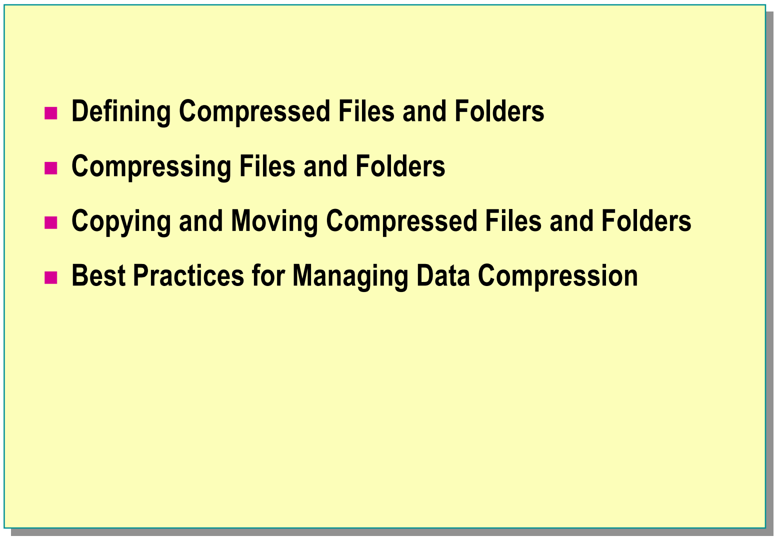
You cannot convert the Windows XP Professional boot volume while Windows XP Professional is running, nor can you force a dismount of the volume that contains a paging file. A *paging* file is a temporary file space that is used for virtual memory. In these situations, you must schedule the conversion to occur the next time that you start Windows XP Professional.

If you must restart the computer to complete the conversion, Windows XP Professional provides a ten second delay before the conversion begins. If you let the conversion proceed, Windows XP Professional must restart twice to complete the conversion.

# ◆ Managing Data Compression

Topic Objective
To introduce how to manage NTFS data compression.

Lead-in
Compressing files and folders enables you to store greater amounts of data in less space.



- Defining Compressed Files and Folders
- Compressing Files and Folders
- Copying and Moving Compressed Files and Folders
- Best Practices for Managing Data Compression

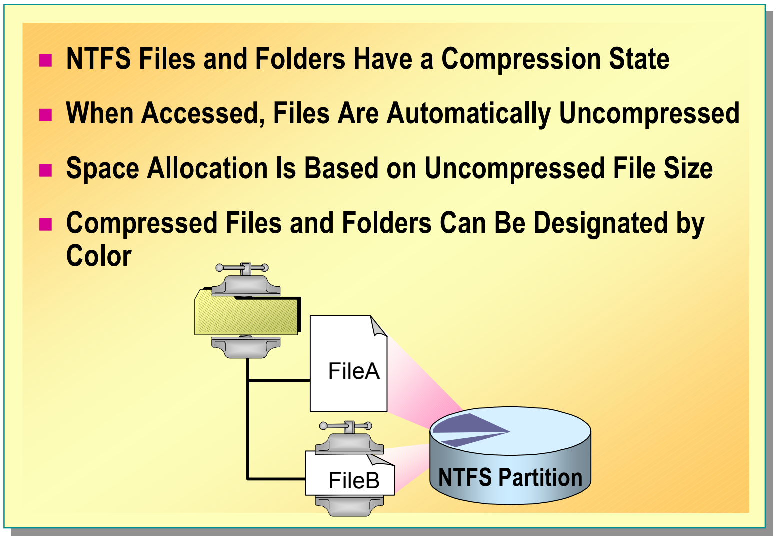
Compressed files and folders occupy less space on an NTFS-formatted volume, thus enabling you to store more data. You can designate the compression state of files and folders as either compressed or uncompressed.

Also, files and folders that you copy or move can retain their compression states, or they can assume the compression state of the target folder to which they are copied or moved. There are best practices for managing data compression that you should follow.

Defining Compressed Files and Folders

Topic Objective
To describe compressed files and folders.

Lead-in
In NTFS both files and folders have a compression state.



- NTFS Files and Folders Have a Compression State
- When Accessed, Files Are Automatically Uncompressed
- Space Allocation Is Based on Uncompressed File Size
- Compressed Files and Folders Can Be Designated by Color

Each file and folder on an NTFS volume has a compression state, which is either compressed or uncompressed. The compression state for a folder does not necessarily reflect the compression state of the files and subfolders in that folder. A folder can be compressed, yet all of the files in that folder can be uncompressed. Similarly, an uncompressed folder can contain compressed files. To change the compression state for a file for folder, you must have Write permissions for that file or folder.

Key Points
Encrypted files and folders cannot be compressed.

Uncompressed files can reside in a folder in a compressed state, and compressed files can reside in a folder in an uncompressed state.

NTFS allocates space for uncompressed files and folders based on the uncompressed size of the file or folder when it is copied or moved.

You can compress unencrypted files and folders that are stored on NTFS volumes. You cannot compress encrypted files or folders.

Access to Compressed Files

When you request access to a compressed file by using a program such as Microsoft Word, or an operating system command such as **copy**, Windows XP Professional automatically uncompresses the file. When you close or save the file, Windows XP Professional compresses it again.

Space Allocation Based on Uncompressed File Size

When a compressed file is copied to a compressed folder, it is decompressed, copied in its decompressed state, and then recompressed. Because the file is in an uncompressed state for a period of time, there must be enough space on the destination volume to hold the file in its uncompressed state. If there is not enough space, the file cannot be copied to the volume. If there is not enough for the uncompressed file, you will receive an error message stating that there is not enough disk space for the file.

Note Windows XP Professional, like Windows NT 4.0 and Windows 2000, supports file compression. Because file compression is not supported on cluster sizes above 4 KB, the default NTFS cluster size for Windows XP Professional never exceeds 4 KB.

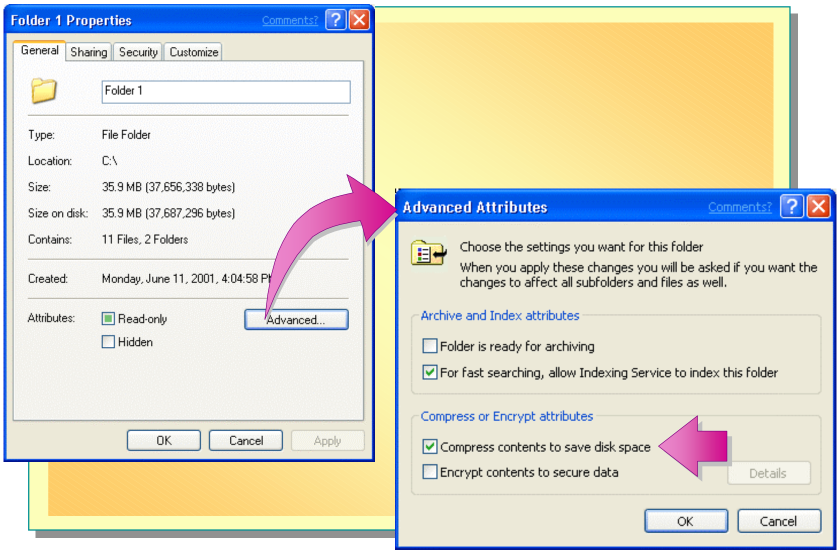
Compression State Display Color

By using Windows Explorer, you can select a different display color for compressed files and folders to distinguish them from uncompressed files and folders.

Compressing Files and Folders

Topic Objective
To describe how to compress files and folders.

Lead-in
By using Windows Explorer, you can set the compression state and change the display color for files and folders.



Folder 1

Type: File Folder

Location: C:\

Size: 35.9 MB (37,656,338 bytes)

Size on disk: 35.9 MB (37,687,296 bytes)

Contains: 11 Files, 2 Folders

Created: Monday, June 11, 2001, 4:04:58 P

Attributes: ■ Read-only
□ Hidden

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

☑ Compress contents to save disk space

□ Encrypt contents to secure data

Delivery Tip
Show students how to set the compression state for a folder. Show students how to set an alternate display color for compressed folders and files.

In Windows XP Professional, you can use Windows Explorer, to set the compression state of files and folders.

To compress a file or folder:

1. Right-click a file or folder, and then select **Properties**.
2. In the **Properties** dialog box, click the **Advanced** button.
3. In the **Advanced Attributes** dialog box, select the **Compress contents to save disk space** check box.

If you compress a folder, the **Confirm Attribute Changes** dialog box appears. This dialog box has two additional options described in the following table.

Option	Description
Apply changes to this folder only	Compresses only the folder that you have selected, but not the files within it. Any files or folders that are later added to it are compressed.
Apply changes to this folder, subfolders and files	Compresses the folder and all subfolders and files that are contained within it and added to it.

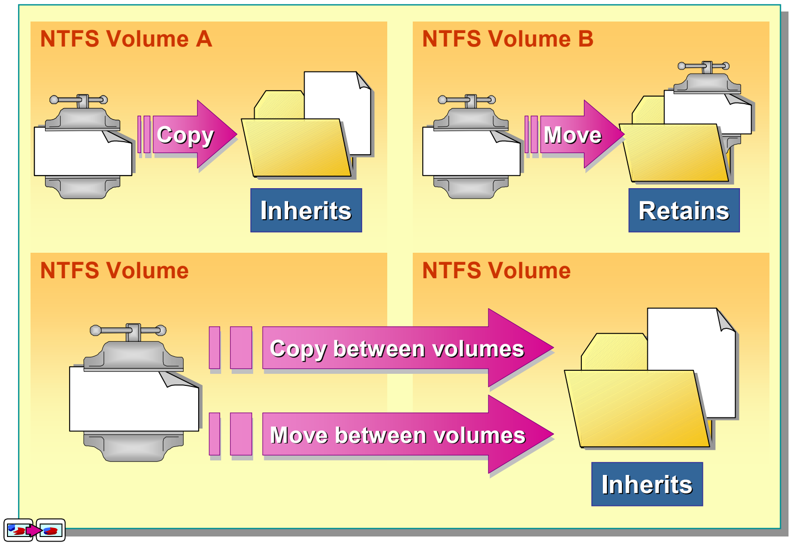
You can set an alternate display color for compressed files and folders.

1. In Windows Explorer, on the **Tools** menu, click **Folder Options**.
2. On the **View** tab, select the **Show encrypted or compressed NTFS files in color** check box, and then click **OK**.

Copying and Moving Compressed Files and Folders

Topic Objective
To explain compression of files and folders that are copied and moved within and between volumes.

Lead-in
Certain rules determine whether the compression state of files and folders is retained when you copy or move them within and between NTFS and non-NTFS volumes.



Delivery Tip
The slide for this topic is animated. Begin by explaining to students how the compression state of a file inherits the compression state of the target folder.

When copying a file or folder within a volume, the file or folder inherits the compressed or uncompressed state of the target folder. When moving a file or folder within a volume, the file or folder retains the original compression state regardless of the state of the target folder. When moving or copying between volumes, the file or folder inherits the state of the destination folder. The following table lists the possible copy and move options and how Windows XP Professional treats the compression state of a file or folder:

Action	Result
Copy a file or folder within a volume	Inherits compression state of the destination folder
Move a file or folder within a volume	Retains original compression state of the source
Copy a file or folder between volumes	Inherits compression state of the destination folder
Move a file or folder between volumes	Inherits compression state of source file or folder

When you move files and folders between volumes, Windows XP Professional first copies the files and folder to the new location, and then deletes them from the original location. When the move is complete, the files inherit the compression state of the target folder.

When you move or copy a compressed file or folder to a non-NTFS volume or disk, Windows XP Professional stores the file or folder as uncompressed.

Note Compression works the same on basic and dynamic disks.

Best Practices for Managing Data Compression

Topic Objective
To present best practices for managing NTFS compression.

Lead-in
Review this checklist before you compress files and folders on NTFS volumes.

☑ **Determine Which File Types to Compress**

☑ **Avoid Compressing System or Executable Files**

☑ **Compress Static Data Rather Than Data That Changes Frequently**

☑ **Use Different Display Colors for Compressed Files and Folders**

Consider the following best practices for managing compression on NTFS volumes:

- Because some file types compress to smaller sizes than others, compress those files that will yield a larger file size reduction. For example, because bitmap files in Windows contain more redundant data than application executable files, this file type compresses to a smaller size. Bitmaps will often compress to less than 50 percent of the original file size, while application files rarely compress to less than 75 percent of the original size.
- Compressing executable files, including system files, will provide little additional space and in most cases will reduce system performance.
- Compress static data rather than data that changes frequently. Compressing and uncompressing files can slow system performance. By compressing files that are accessed infrequently, you minimize the amount of system time that is dedicated to compression and uncompression activities.
- To make it easier to locate compressed data, use different display colors for compressed folders and files.

Lab 13A: Configuring Disk Compression

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will configure a volume for compression, and move and copy compressed files.

Objectives

After completing this lab, you will be able to:

- Configure an NTFS volume for compression.
- Move files with the compression attribute set.
- Copy files with the compression attribute set.

Prerequisites

Before working on this lab, you must have:

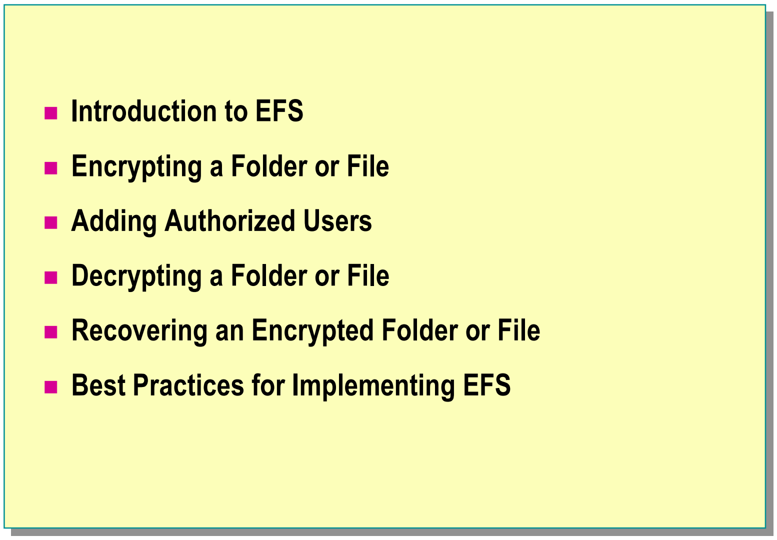
- Knowledge of the NTFS file system.
- Knowledge of file compression.

Estimated time to complete this lab: 15 minutes

# ◆ Securing Data by Using EFS

Topic Objective
To describe the benefits of encryption.

Lead-in
EFS, built into the NTFS file system in Windows XP, enables public key-based protection at the file or folder level.



- Introduction to EFS
- Encrypting a Folder or File
- Adding Authorized Users
- Decrypting a Folder or File
- Recovering an Encrypted Folder or File
- Best Practices for Implementing EFS

Key Points
When a file’s encryption attribute is on, EFS saves any changes transparently as encrypted data.

Security features such as logon authentication protect network resources from unauthorized access. However, if an attacker has physical access to a computer (for example, a stolen notebook computer), it is fairly easy to install a new operating system and bypass the existing operating system's security. This leaves sensitive data exposed. Users can add an effective layer of security by encrypting these files by using the Encrypting File System (EFS). When the files are encrypted, the data is protected even if an attacker has full access to the computer’s data storage.

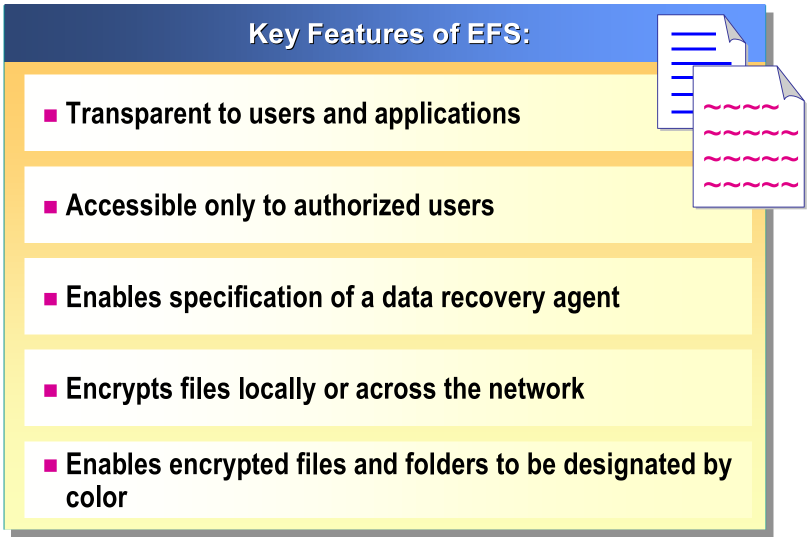
EFS provides file-level encryption for NTFS files. When a file’s encryption attribute is on, EFS stores the file as encrypted. When an authorized user opens an encrypted file in an application, EFS decrypts the file in the background and provides an unencrypted copy to the application. From the user’s point of view, encrypting a file is simply a matter of setting a file attribute. The authorized users can view or modify the file, and EFS saves any changes transparently as encrypted data. The unauthorized user receives the message Access Denied when attempting to access an encrypted file.

EFS is especially useful for securing sensitive data on portable computers or on computers that are shared by several users. In a shared system, an attacker can gain access by starting up a different operating system such as MS-DOS from a floppy disk. Also, a portable computer can be stolen, and the thief can then remove the hard disk drive, plug it into another computer, and read the files. EFS files, however, appear as unintelligible characters when the attacker does not have the decryption key.

Introduction to EFS

Topic Objective
To identify the key features of EFS.

Lead-in
EFS enables users to store their data on the hard disk in encrypted format.



Key Features of EFS:

- **Transparent to users and applications**
- **Accessible only to authorized users**
- **Enables specification of a data recovery agent**
- **Encrypts files locally or across the network**
- **Enables encrypted files and folders to be designated by color**

Key Points
A file remains encrypted for as long as it is stored on disk.

Encryption and compression are different processes. Files cannot be encrypted and compressed at the same time.

EFS enables users to store data on the hard disk in encrypted format. After a user encrypts a file, the file remains encrypted for as long as it is stored on disk. Note that encryption and compression are different processes. Files cannot be encrypted and compressed at the same time.

EFS has several key features:

- It operates in the background and is transparent to users and applications.
- It enables only authorized users to gain access to an encrypted file. EFS automatically decrypts the file for use and then encrypts the file again when it is saved.
- Authorized data recovery agents can recover data that was encrypted by another user. A data recovery agent is a user account that is configured for the recovery of encrypted files. Data recovery agents ensure that data is accessible if the user that encrypted the data is unavailable or loses his or her private key. However, in Windows XP Professional data recovery agents are not required for EFS to operate.
- Files can be encrypted locally or across the network. Files in offline folders, Client-side Caching, can be encrypted.
- Enables display color to designate encrypted files and folders.

Because EFS operates at the system level, it can save temporary files to non-EFS protected folders. For greater protection, consider encrypting at a folder level. All files that are added to EFS protected folders are encrypted automatically.

EFS does not encrypt data as it is transmitted over the network. Because data is transmitted as plaintext, EFS should not be implemented as the basis of network security for files. To secure data as it is transmitted, consider:

Key Points
EFS does not encrypt data as it is transmitted over the network.

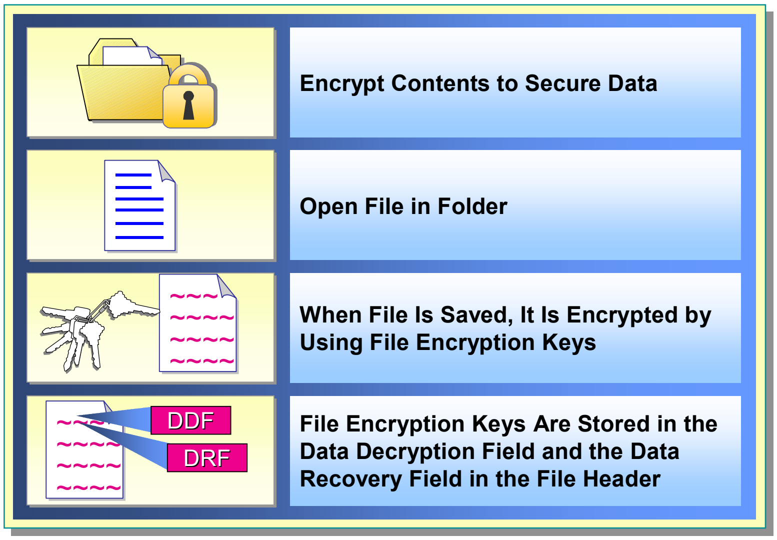
- Implementing EFS broadly on local computers and then using Internet Protocol security (IPSec) to encrypt data as it travels over the network.
- Using Web Distributed Authoring and Versioning (WebDAV) which encrypts files as they are transmitted. When files are retrieved from WebDAV folders, the files are transmitted as *raw data streams*. This means that the file is not decrypted before it is transmitted. For more information on WebDAV, see Course 2295A, *Implementing and Supporting Microsoft Internet Information Services 5.0.*
- Storing encrypted files by using Remote Desktop or Terminal Services and allow access only over remote sessions.

Note EFS is supported only for versions of NTFS for Windows 2000 and Windows XP. It does not work with any other file system, including versions of NTFS running on Windows NT.

Encrypting a Folder or File

Topic Objective
To discuss the purpose and benefit of encryption keys and illustrate the procedure for encrypting files and folders on an NTFS **volume**.

Lead-in
A file is encrypted by using file encryption keys.



Encrypt Contents to Secure Data

Open File in Folder

When File Is Saved, It Is Encrypted by Using File Encryption Keys

File Encryption Keys Are Stored in the Data Decryption Field and the Data Recovery Field in the File Header

EFS encrypts a file or folder as follows:

1. All data streams in the file are copied to a plaintext temporary file in the system's temporary directory.
2. A file encryption key is randomly generated and used to encrypt the data by using an encryption algorithm.
3. A Data Decryption Field (DDF) is created to contain the file encryption key and the user’s public key. EFS automatically obtains the user’s public key from the user’s file encryption certificate. A *certificate* is a digital document commonly used for authentication, and is signed and issued by a certification authority. Each user has a personal certificate store created when a user is added to the system. The certification authority can issue additional certificates.
4. If a recovery agent has been designated through Group Policy, a Data Recovery Field (DRF) is created to contain the file encryption key and the recovery agent’s public key. EFS automatically obtains the recovery agent’s public key from the recovery agent’s file recovery certificate, which is stored in the Encrypted Data Recovery Policy. If there are multiple recovery agents, the file encryption key is encrypted with each agent’s public key, and a DRF is created to store each encrypted file encryption key.
5. EFS writes the encrypted data, along with the DDF and the DRF, back to the file.
6. The plaintext temporary file is deleted.

All files and subfolders that you create in an encrypted folder are also automatically encrypted. Each of these files has a unique encryption key, which makes it safe for you to rename files. If you move a file from an encrypted folder to an unencrypted folder on the same volume, the file remains encrypted.

Encrypting a File or Folder

To encrypt a file or folder:

1. Right-click the file or folder, and then click **Properties**.
2. Click the **General** tab, and then click **Advanced**.
3. Click **Encrypt contents to secure data**.

   When you click **OK**, if the folder contains unencrypted files or subfolders, a **Confirm Attribute Changes** dialog box appears and gives you the option to apply the changes to the folder only, or to the folder, its subfolders, and all files.

Encrypting Files That You Do Not Own

EFS enables you to encrypt files that you do not own, provided that you have Write Attributes, Create Files/Write Data, and List Folder/Read Data permissions for the files.

If you select **Encrypt contents to secure data** and the **Confirm Attribute Changes** dialog box appears, and you choose the **Apply changes to this folder, subfolders and files** option, only you will be able to decrypt the files; other users will not be able to access the files and folders.

If there are files encrypted that you need to have decrypted, you can recover the files by:

- Selecting the individual folders to decrypt and clearing the **Encrypt contents to secure data** check box.

Viewing the Encryption Status of a File or Folder

Because encryption is an attribute of a file or folder, it is possible to determine whether a file or folder is already encrypted by examining its attributes. You can also add the **Attributes** column to the **Details** view. Therefore, you will see that any file or folder with an **E** attribute is encrypted.

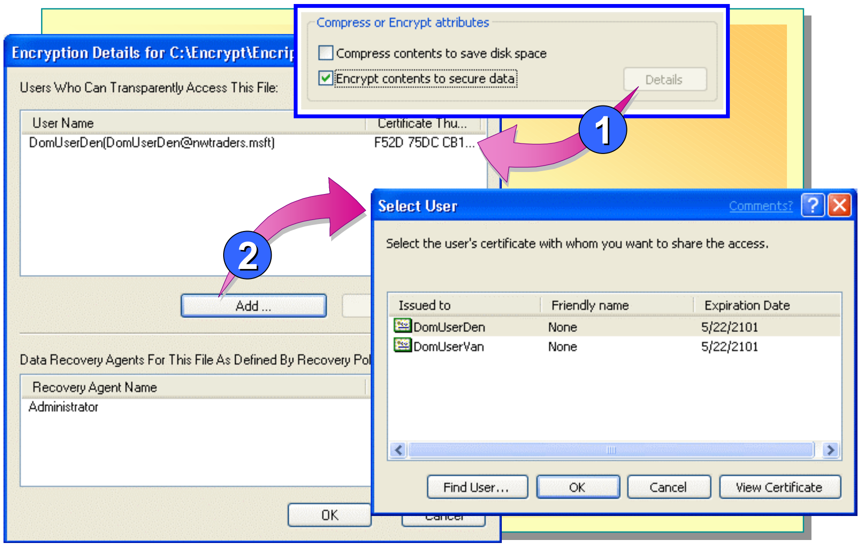
You can also indicate encrypted folders by using an alternate display color. To set an alternate display color for encrypted folders:

1. In Windows Explorer, on the **Tools** menu, click **Folder Options**.
2. On the **View** tab, select the **Show encrypted or compressed NTFS files in color** check box, and then click **OK**.

Adding Authorized Users

Topic Objective
To describe authorizing additional users to access encrypted files.

Lead-in
You can designate additional users to access encrypted files.



Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

Encryption Details for C:\Encrypt\Encrip

Users Who Can Transparently Access This File:

User Name	Certificate Thu...
DomUserDen(DomUserDen@nwtraders.msft)	F52D 75DC CB1...

Data Recovery Agents For This File As Defined By Recovery Pol

Recovery Agent Name
Administrator

Select User

Select the user's certificate with whom you want to share the access.

Issued to	Friendly name	Expiration Date
DomUserDen	None	5/22/2101
DomUserVan	None	5/22/2101

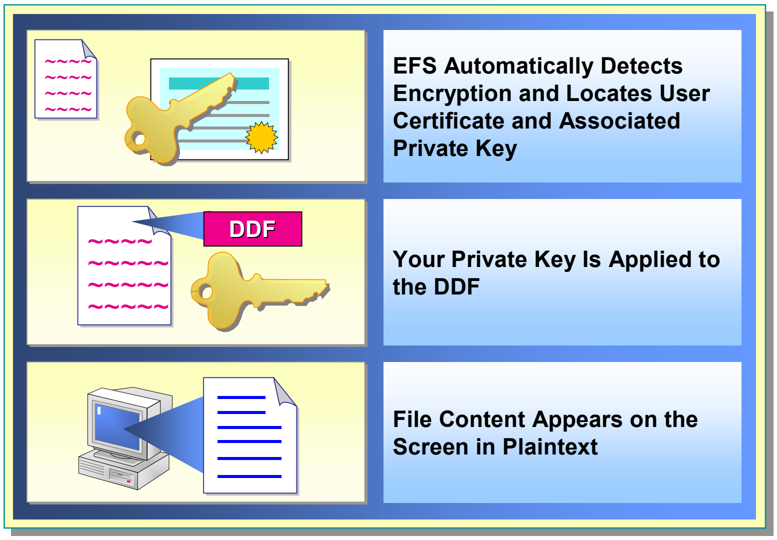
When adding an authorized user to an EFS encrypted file, you can add a domain user or a trusted domain user. However, before a user can be added, that user must have a valid EFS certificate in the Active Directory™ directory service.

After you encrypt a file, open the property sheet of the file, click **Advanced**, and then click **Details** to add additional authorized users. The **Encryption Details** sheet displays authorized users in the upper pane and designated data recovery agents in the lower pane. Only authorized users can be added on this sheet.

Decrypting a Folder or File

Topic Objective
To describe how to decrypt files and folders on an NTFS volume.

Lead-in
You can decrypt a folder or file on an NTFS volume by using your private key.



EFS Automatically Detects Encryption and Locates User Certificate and Associated Private Key

Your Private Key Is Applied to the DDF

File Content Appears on the Screen in Plaintext

When applications need to gain access to an encrypted file, the file must be decrypted. Decryption proceeds as follows:

1. NTFS recognizes the file is encrypted and sends a request to EFS.
2. EFS retrieves the DDF (Data Decryption Field).
3. EFS retrieves the user’s private key from the user’s profile and uses it to decrypt the DDF and obtain the file encryption key.
4. EFS uses the file encryption key to decrypt sections of the file as needed for the application.
5. EFS returns the decrypted data to NTFS, which then sends the data to the requesting application.

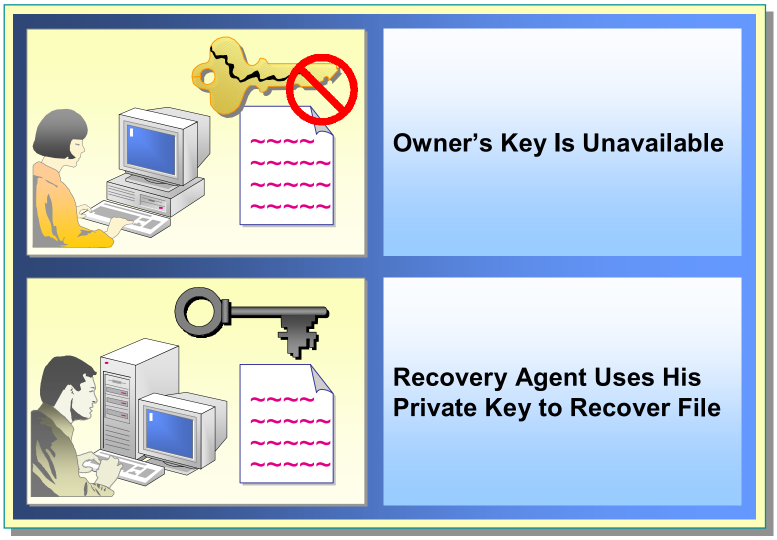
To remove encryption from a file or folder:

1. Right-click the file or folder, and then click **Properties**.
2. Click the **General** tab, and then click **Advanced**.
3. Clear the **Encrypt contents to secure data**.

Recovering an Encrypted Folder or File

Topic Objective
To explain the process of EFS recovery.

Lead-in
If the owner loses the private key, the recovery agent can still recover the encrypted file.


Owner's Key Is Unavailable

Recovery Agent Uses His Private Key to Recover File

If the owner's private key is unavailable, a designated recovery agent can open the file by using his or her own private key. If the recovery agent is using another computer on the network, you must send the file to the recovery agent. The recovery agent can bring his or her private key to the owner's computer, but copying a private key onto another computer is not a recommended security practice. The default recovery agent is the Administrator account for the local computer.

Key Points
Data Recovery Agents are user accounts.

One or more users, typically administrator-level accounts, can be designated as data recovery agents through Local Policy on stand-alone computers or through Group Policy in a domain.

If the recovery agent designation changes, then access to the file is denied. For this reason, it is recommended that you keep recovery certificates and private keys until all files that are encrypted by using those recovery certificates and private keys have been updated.

One or more users, typically administrator-level accounts, can be designated as data recovery agents through Local Policy on stand-alone computers or through Group Policy in a domain. Data Recovery Agent (DRAs) are issued recovery certificates with public and private keys that are used for EFS data recovery operations. By default, in a domain, the EFS recovery policy designates the highest-level administrator account as the DRA on the first domain controller installed in the domain. Different DRAs can be designated by changing the EFS recovery policy, and different recovery policies can be configured for different parts of an enterprise.

Note In Windows 2000, DRAs were required to implement EFS. In Windows XP, they are optional. Microsoft recommends that all stand-alone or domain environments have at least one designated DRA.

Backing Up and Restoring Encrypted Files or Folders

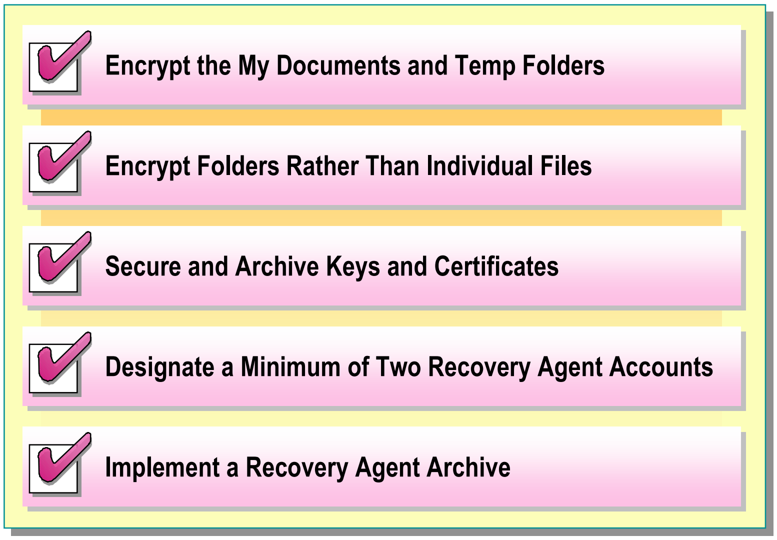
Encrypted files and folders remained encrypted when you back them up. Backup files remain encrypted when transferred across the network or when copied or moved onto any storage medium, including non-NTFS volumes. If you restore backup files to NTFS volumes in Windows 2000 or Windows XP, they remain encrypted. Along with providing effective disaster recovery, backups can also be used to securely move files between computers and sites.

Opening restored, encrypted files is no different from decrypting and opening any other encrypted files. However, if files are restored from backup onto a new computer, or at any location where the user's profile, and thus the private key that is needed to decrypt the files, is not available, the user can import an EFS certificate and private key. After importing the certificate and private key, the user can decrypt the files. A data recovery agent can also be used to decrypt a file for the user, if the user is unable to decrypt the file.

Best Practices for Implementing EFS

Topic Objective
To review best practices for implementing EFS.

Lead-in
Like any security process, encryption should be planned, including deciding which files and folders to encrypt, which permissions to grant, and how to handle encryption backup and archival.



- ✓ Encrypt the My Documents and Temp Folders
- ✓ Encrypt Folders Rather Than Individual Files
- ✓ Secure and Archive Keys and Certificates
- ✓ Designate a Minimum of Two Recovery Agent Accounts
- ✓ Implement a Recovery Agent Archive

Encryption is a sensitive operation. It is important that encrypted data not become inadvertently decrypted. To this end, it is recommended that users do the following:

- Encrypt the My Documents folder (*RootDirectory*\UserProfile\\My Documents) to ensure that personal folders where most Microsoft Office documents are saved are encrypted by default. Encrypt the Temp folder (*RootDirectory*\\Temp) to ensure that any temporary files created by various applications are encrypted, and prevents any sensitive data from being disclosed.
- Encrypt folders rather than individual files. Applications use files in various ways; for example, some applications create temporary files in the same folder during editing. These temporary files may or may not be encrypted, and some applications substitute these temporary files for the original files when the edits are saved. Encrypting at the folder level ensures that files do not get decrypted when the temporary files are used.
- Export the private keys for recovery accounts, store them in a safe place on secure media, and remove the keys from local computers. These steps prevent someone from using the recovery account on the computer to read files that are encrypted by other users. This is especially important for stand-alone computers where the recovery account is the local administrator or another local account. For example, a portable computer that contains encrypted files might be stolen, but if the private key for recovery is not on the computer, the thief cannot log on by using the recovery account and then use it to recover files.

- Designate a minimum of two recovery agent accounts for EFS recovery use Do not use the recovery agent account for any other purpose than its intended use, that is, routine access to other user’s files.
- Do not destroy recovery certificates and private keys when recovery agent policy changes. Keep them in archives until you are sure that all files that are protected by these certificates and keys have been updated by using new recovery agent information. Recovery certificates and private keys must be exported and stored in a controlled and secure manner. It is recommended that you store archives in a controlled-access vault, and that you have a master archive and a backup archive. The master archive should be placed in a secure onsite location, and the backup archive placed in a secure offsite location.

Lab 13B: Securing Files by Using EFS

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will encrypt and decrypt a file.

Objectives

After completing this lab, you will be able to:

- Encrypt a file.
- Share an encrypted file.
- Decrypt a file.

Prerequisites

Before working on this lab, you must have:

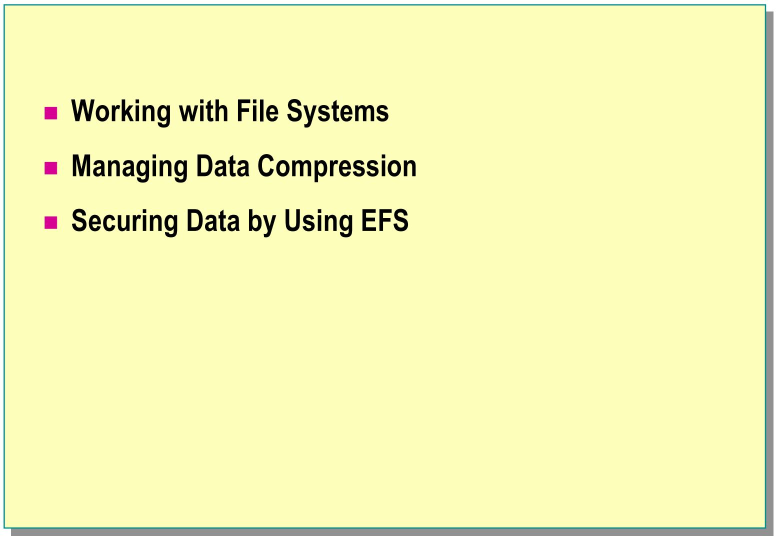
- Basic knowledge of file encryption.
- Basic knowledge of Active Directory.

Estimated time to complete this lab: 30 minutes

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.



- Working with File Systems
- Managing Data Compression
- Securing Data by Using EFS

1. A user shares a computer with other users. The user attempts to gain access to a file on the computer's local drive and receives an Access Denied message. After verifying that the NTFS permissions allow the user Full Control, what is causing the Access Denied message to display? How can the user obtain access to the file?

   The file is encrypted with EFS. If a user needs access to the file, the individual who encrypted the file must decrypt the file. The alternative is to send the encrypted file to a designated recovery agent to decrypt the file.

2. You are installing 10 new computers running Windows XP Professional. Workers on different shifts will share these computers. It has been decided that all user data will be stored on the local computers hard disk. Each user’s My Documents folder needs to be accessible by only that user. How should you configure these computers?

   You would configure these computers using the NTFS file system. The My Documents folders are automatically secured when using NTFS.

3. After upgrading your computers from Windows 98 to Windows XP Professional you have decided to take advantage of the expanded features of the NTFS file system. You need to accomplish this with the least amount of administrative effort, and also need to maintain the user’s data. What should you do to accomplish these goals?

   Use the Convert utility. The command would be convert c: /FS:NTFS.

4. A user stores a very large number of graphic files on a local disk. For security purposes, it has been decided that these files are to be stored only on that user's computer. The user reports that Windows XP Professional is displaying a message that the C: drive is running out of disk space. You have verified that the disk has no remaining unformatted free space. What can you do to help this user?

   Use NTFS compression to compress the folders containing the graphic files. These files are likely to compress to a much smaller percentage of space used.

5. A user has created a folder on drive D to archive old files. They have used NTFS compression on the folder. The user calls you to ask why, when some files are moved to the compressed folder, they are compressed when others aren't. What do you tell the user?

   When files are moved from the C: drive to the D: drive, they inherit the compression attribute of the new folder. When files are moved from one place on the D: drive to another, the compression attribute is maintained from the original folder.

6. One of your traveling sales representatives has a laptop running Windows XP Professional as a member of an Active Directory domain. The sales representative maintains confidential data on the laptop. For security purposes, these files are kept encrypted. The user is unable to attend a conference, and plans to send an assistant to the conference. The assistant needs temporary access to some of the encrypted files. How do you provide temporary access to the assistant?

   Have the user add the assistant as an authorized user to these encrypted files.