# *File System*

## Section Seven

**NTFS, EFS, Partitioning, and Navigating Folders**

## *NTFS*

**DEFINITION**

New Technologies File System or NTFS was first applied in Windows NT 3.0 back in 1992. This technology has pretty much stayed the same ever since.

When a hard disk is formatted (initialized), it is divided into partitions or major divisions of the total physical hard disk space. Within each partition, the operating system keeps track of all the files that are stored by that operating system. Each file is actually stored on the hard disk in one or more clusters or disk spaces of a predefined uniform size. Using NTFS, the sizes of clusters range from 512 bytes to 64 kilobytes. Windows NT provides a recommended default cluster size for any given drive size. For example, for a 4 GB (gigabyte) drive, the default cluster size is 4 KB (kilobytes). Note that clusters are indivisible. Even the smallest file takes up one cluster and a 4.1 KB file takes up two clusters (or 8 KB) on a 4 KB cluster system.

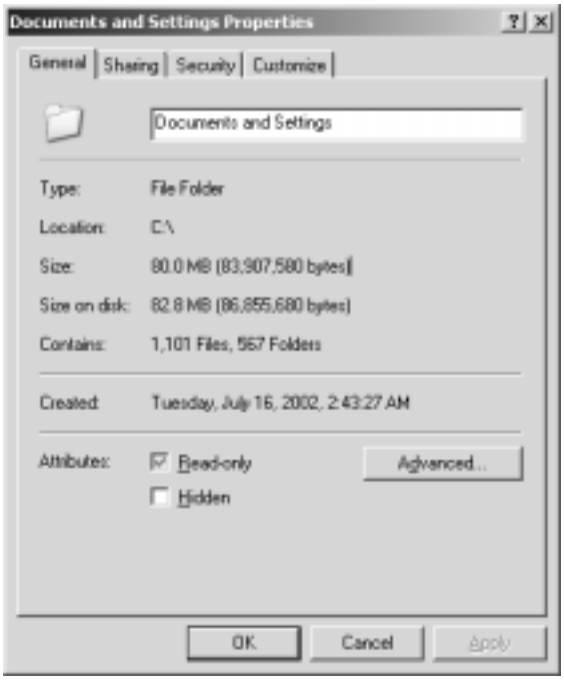
The selection of the cluster size is a trade-off between efficient use of disk space and the number of disk accesses required to access a file. In general, using NTFS, the larger the hard disk the larger the default cluster size, since it's assumed that a system user will prefer to increase performance (fewer disk accesses) at the expense of some amount of space inefficiency.

When a file is created using NTFS, a record about the file is created in a special file, the Master File Table (MFT). The record is used to locate a file's possibly scattered clusters. NTFS tries to find contiguous storage space that will hold the entire file (all of its clusters).

**SECURITY**

NTFS provides much more security then that of FAT32[1]. While FAT32 offers READ, WRITE, EXECUTE options for files and folders on the hard drive, NTSF offers an extensive array of limiting options for you to apply to your files and folders (shared or unshared). NTFS also allows you the ability to encrypt files and folders so that no one (except the owner) can gain access, copy or delete content.

**FIGURE 1. Folder Properties**




Within folder settings (any folder in NTFS), additional options are available:

- Security tab
- Advanced attributes

## THE SECURITY TAB

The Security tab provides advanced settings for how people access files. It should be noted here that what is set in the NTFS DACL[1] overrides all other access permission (including the shared files and folders options). What you set in the NTFC securities

1. FAT32 provides the following enhancements over previous implementations of the FAT file system:

   FAT32 supports drives up to 2 terabytes in size.

   **NOTE**: Microsoft Windows 2000 only supports FAT32 partitions up to a size of 32 GB.

   FAT32 uses space more efficiently. FAT32 uses smaller clusters (that is, 4-KB clusters for drives up to 8 GB in size), resulting in 10 to 15 percent more efficient use of disk space relative to large FAT or FAT16 drives.

   FAT32 is more robust. FAT32 can relocate the root folder and use the backup copy of the file allocation table instead of the default copy. In addition, the boot record on FAT32 drives is expanded to include a backup copy of critical data structures. Therefore, FAT32 drives are less susceptible to a single point of failure than existing FAT16 drives.

   FAT32 is more flexible. The root folder on a FAT32 drive is an ordinary cluster chain, so it can be located anywhere on the drive. The previous limitations on the number of root folder entries no longer exist. In addition, file allocation table mirroring can be disabled, allowing a copy of the file allocation table other than the first one to be active. These features allow for dynamic resizing of FAT32 partitions. Note, however, that although the FAT32 design allows for this capability, it will not be implemented by Microsoft in the initial release.

options should be the base minimum for access to any given file or folder because it applies to direct access as well as indirect (or remote) access. Only limit access as needed and always try to not use the DENY option unless it unavoidable.

## ADVANCED SECURITY SETTINGS

**FIGURE 2. Advanced Security Settings**


In the Advanced Securities Settings dialog box there are four main tabs:

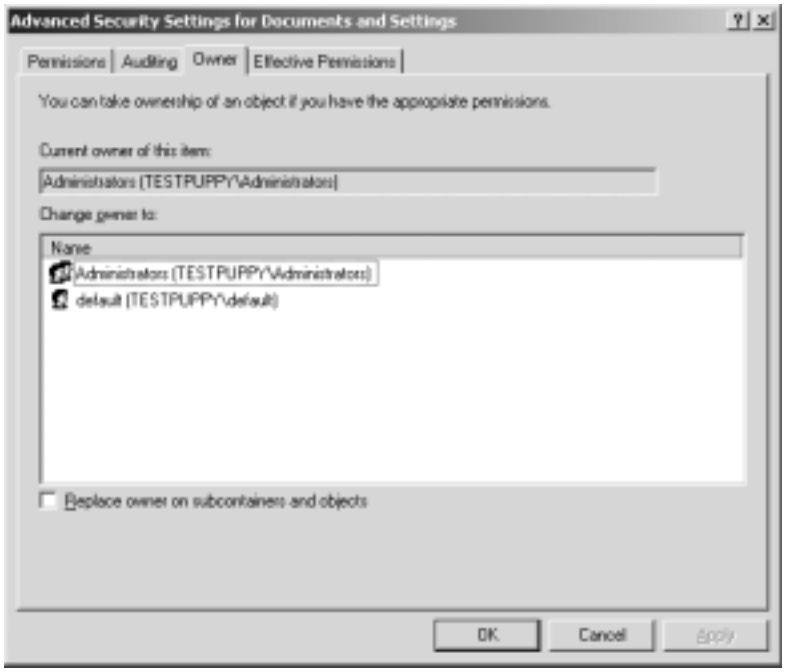
1. Permission
2. Auditing
3. Owner
4. Effective Permission

For purposes of simplicity we will look at Ownership and Effective Permission.

1. Every Active Directory object has associated with it a *security descriptor* property that protects the object. Within the security descriptor you can control a *discretionary access control list* (DACL) that in turn contains a list of *access control entities* (ACEs). It's those ACEs that protect the object. Each ACE grants or denies access to specified property of the object to a user or group. If you're interested in the gory details, see the Access Control Model page on the Microsoft Developer's site, which provides links to some great detailed discussions of the mechanisms at work, including the interaction between threads and securable objects.

## OWNER

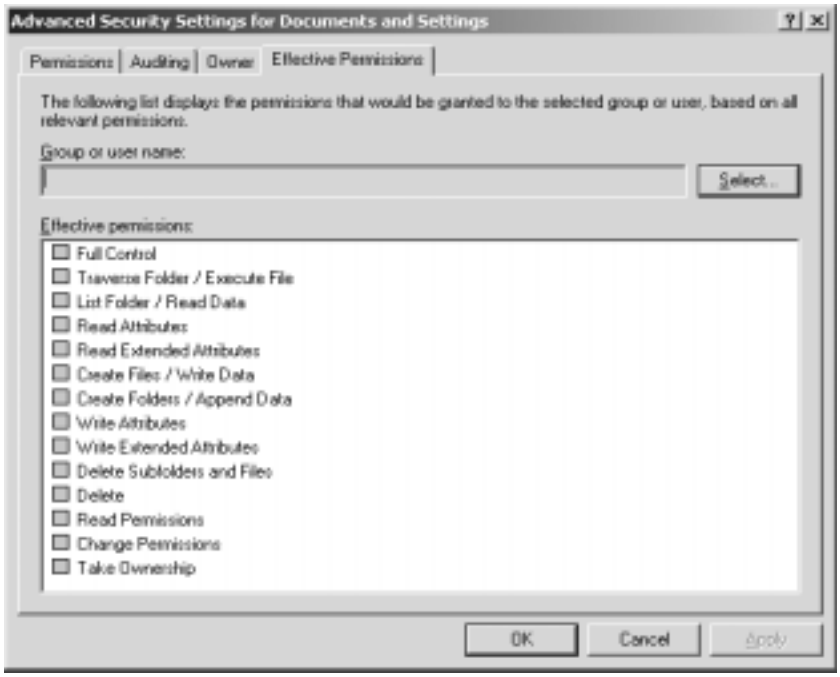
**FIGURE 3. Owner Properties**




Owner properties displays who created the folder or file. In this, only the Administrator (or someone with administrative rights) can take ownership of files. In XP Administrators can take ownership of encrypted files and folder but can not open or alter their content.

## EFFECTIVE PERMISSION

**FIGURE 4. Effective Permission Properties**



As you can see, effective permission are much more exacting. They cover a much more robust file security that can share data (or not) with greater control.

## FOLDER OPTIONS

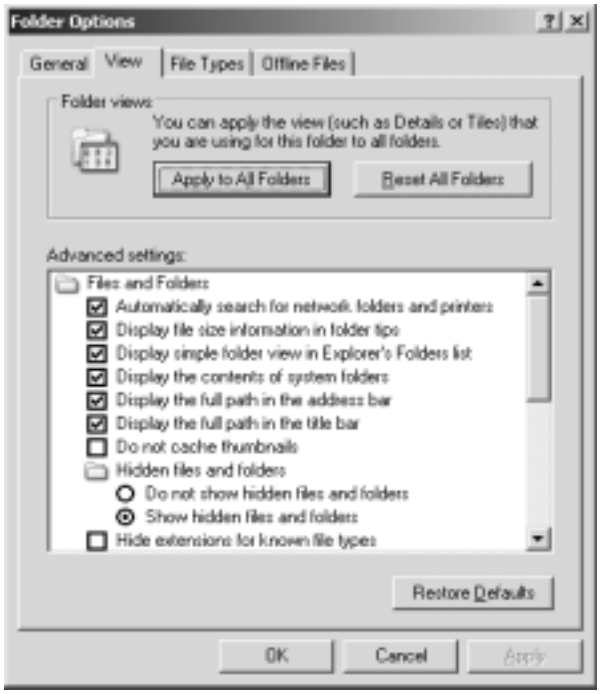
Although Windows XP Professional is geared for advanced users, Microsoft enabled several options intended to simplify the user interface. However, many advanced users may find the default settings distracting.

Default settings are particularly distracting in Windows Explorer. The first thing advanced Windows XP users may want to do is to change the view from the Tiles to the Details setting. Other default settings are located on the Folder Options dialog (Select Folder Options from the Tools menu).

The following are additional settings that you may want to change. They are located on the View tab:

- **Display The Contents Of System Folder**: By default, this setting is disabled. You may want to enable it.
- **Display Simple Folder View In Explorer's Folder List**: If you don't like the new appearance of the Folder list (it doesn't display dotted lines and underlines every folder you click), then turn off these settings.
- **Show Hidden Files And Folders**: By default, Windows XP hides the hidden files and folders from you.
- **Hide Extensions For Known File Types**: Disable this setting and see the extensions of all files.
- **Hide Protected Operating System Files (Recommended)**: If you want to see all of the files on your hard drive, turn this setting off.
- **Show Control Panel In My Computer**: You may want to turn this on.

**FIGURE 5. Folder Options properties**



**Use Simple File Sharing (Recommended)**: Even though Windows XP recommends leaving this setting on, you may want to turn it off. If you leave it off, you'll get a simplified user interface on the Security and Sharing tab. If you previously worked with Windows NT and 2000, the interface will only confuse you.

## IMPORTANT THINGS TO KNOW ABOUT EFS

Windows XP's Encrypting File System (EFS) can help you secure important files. Even though EFS shipped almost three years ago with Windows 2000, it's still very safe. Since its inception, EFS has not been hacked; however, this doesn't mean you are safe from attack. You still must configure and manage EFS and follow security best practices.

The first thing you should do is ensure that your users are using effective passwords. If they aren't, EFS won't help. No technology can help if passwords are weak. For instance, EFS can encrypt files, but if an attacker gets to a user's password, the hacker can access the user's EFS encrypted files. There's no need to hack EFS if you can obtain another user's password.

Secondly, users should export their certificates and keep them in a secure place. If certificates fall into the wrong hands, EFS security is breached. You'll also have problems if you lose your certificate. This is true, for instance, if you encrypt files but forget to export the certificate and then reinstall the operating system. If you used a local account, your files would be lost, and would not be retrievable. Always remember to export the certificate and keep it in a safe place.

EFS is a very important feature. If you use it on your computer, make sure you read everything about it in the Help and Support Center. (EFS is available only in Windows XP Professional.)

**FIGURE 6. Encryption Option (advanced attributes)**


## COMPARING EFS IN WIN2K AND WINXP

Encrypting File System (EFS) allows you to encrypt your files and thus prevent other users from seeing the files' content. The first version of EFS was built into Windows 2000. Although Windows XP is a minor upgrade from Windows 2000, you should be aware of the following important changes in EFS:

- Only Windows XP Professional includes EFS. (The Home Edition doesn't.)

- By default, Windows 2000 includes a default Recovery Agent. (Windows XP Professional in a workgroup doesn't, but Windows XP joined to a domain does.)
- In Windows 2000, you can disable EFS by deleting the Recovery Agent. In Windows XP, deleting the RA doesn't disable EFS.
- To disable EFS in Windows XP in a workgroup, you must change a registry entry (HKLM\Software\Microsoft\Windows NT\CurrentVersion\Efs\EFSconfiguration to 1).
- To disable EFS on Windows XP in a domain environment, you have to change the Group Policy setting.
- Windows XP allows you to share encrypted files. Windows 2000 doesn't support this feature.

**Note:** Please remember that editing the registry is potentially dangerous. Always have a backup before you begin.

### TWO WAYS TO DISABLE EFS

When Windows XP is configured in workgroup environments, by default it doesn't use Recovery Agent. Therefore, disabling EFS in Windows XP is handled differently than in Windows 2000. There are two ways to disable EFS, depending on the configuration.

1. If your computer is joined to a domain, you can disable EFS through Group Policy:
2. Open the Group Policy at the level you want to disable EFS.
3. Go to Computer Configuration | Windows Settings | Security Settings/.
4. Expand the Public Key Policies.
5. Right-click the Encrypting File System and click Properties.
6. Remove the check from Allow Users To Encrypt Files Using Encrypting File Systems (EFS).
7. Exit the console.

If your computer is not joined to a domain, this Group Policy setting has no effect. Instead, you'll need to manually change the registry:

1. Open the registry editor (Regedit.exe).
2. Open the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\EFS key.
3. Choose Edit / New. Click the DWORD value.
4. Type EfsConfiguration as the name.
5. Double-click the new value and change its value to 1.
6. Restart the computer.

EFS is available only in Windows XP Professional. It is not available in Windows XP Home Edition.

### EFS BEST PRACTICES

The following are some tips that will help you more efficiently use the Encrypting File System (EFS) in Windows XP:

- Always encrypt folders, not individual files. Many applications (like Word) create temporary files in the same folder. If you encrypt only individual files, the temporary files are not encrypted.
- Encrypt your “My Documents” folder.

- Encrypt%Temp% encamps% folders.
- Export your certificate and private key and keep them in a safe place.
- Export Recovery Agent's certificate and private key and keep them in a safe place.
- If you transfer sensitive data over the network, use IPSec. When you send an EFS encrypted file over the network, the file is decrypted and sent in plaintext. IPSec allows you to encrypt the data for transmission over the network.
- When you print, don't use spool files or encrypt the spool folder.

You cannot encrypt files with system attributes, or files in the %SystemRoot% folder and its subfolders.

### ENCRYPT THE LOCAL COPY OF REMOTE FILES

Windows 2000 ships with a feature called Off-line Files that allows users to access files on a remote computer, even when the network connection is down. The idea behind this technology is very simple: The operating system creates a copy of the network file on the local computer, and when the network connection is down, it uses the local copy. When the connection is up again, it synchronizes the files.

Windows XP Professional has the same technology, but with one additional feature--encryption. It allows you to encrypt the local copy of the remote files. Here's how:

1. Open Windows Explorer, select Tools, and then click Folder Options.
2. Go to the Off-line Files tab. If you don't see any settings, follow the instructions on the dialog box and disable Fast User Switching. Once you do that, you'll see the settings.
3. Select Enable Off-line Files.
4. Select Encrypt Off-line Files To Secure Data.
5. Click OK.

The files will be encrypted with the Encrypted File System (EFS). If you use FAT or FAT32, you won't be able to encrypt the files. EFS is available only on Windows XP Professional partitions formatted with NTFS.

### SHARING HELP FILES

Help and Support Center is more than just a collection of help files. It is an entire help system consisting of several features, including the sharing of help files, which allows help files on one computer to be used on another computer. This is useful if you need to access help files from different versions of your operating system. For example, if you need to access the Windows.NET Server help files, you would share the help files on that system and then use them on your Windows XP computer.

Before you can use the help files on another system, you must first share them.

1. Open Help And Support from the Start menu.
2. Click the Options button on the navigation bar.
3. Click Install And Share Windows Help under the Options section in the left part of the screen.
4. Select Share Your Help Content With Others On Your Network.
5. Select the Shared option, and click Apply.

The help files are now shared. Once you have shared the help files, install them on your computer.

1. Open Help And Support from the Start menu.
2. Click on the Options button on the navigation bar.
3. Click on Install And Share Windows Help under the Options section in the left part of the screen.
4. Select Install Help Content From Another Windows Computer.
5. Type the name of the computer that has shared its help files, and click Find.
6. Select the help files from the remote computer, and click Install.

In the final step, use the help files you installed.

1. Open Help And Support from the Start menu.
2. Click the Options button on the navigation bar.
3. Click Install And Share Windows Help under the Options section in the left part of the screen.
4. Select Switch From One Operating System's Help Content To Another.
5. Select the help files you want to use and click Switch.

The Help and Support Center will now use these files as its Help database.

Sharing help files is a useful feature; however, before using it, you'll need to know some additional facts.

- You can't share help files on older operating systems, such as Windows 2000 or Windows ME. Also, older operating systems can't use Windows XP's shared help files. You can only share help files on Windows XP and newer operating systems.
- You can't use help files from multiple operating systems at the same time. Although you can have several help files installed, you can only use one at any given time. To use another help file, you must switch the help content.

If you've installed help files from Windows XP and Windows.NET Server on your Windows XP computer and you perform a switch from Windows XP to Windows.NET Server help files, the switch is permanent. To go back, you must perform another switch.

Here's a trick for performing a temporary switch:

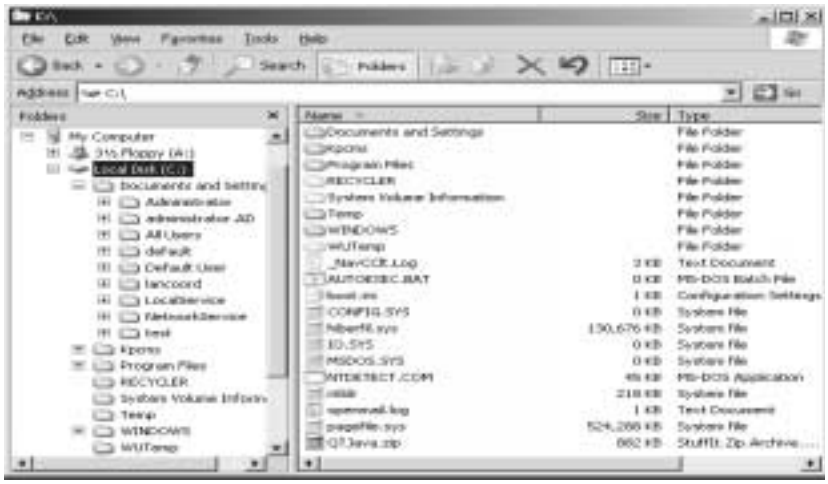
1. Open Help And Support Center from the Start menu.
2. Open another instance of the Help And Support Center.
3. Switch the Help content in this second instance.
4. Use the content.
5. Close the second instance (the window in which you switched the Help content).
6. Close the first instance of Help And Support Center.

It's very important that you close the windows in the correct order. If you fail to do this, you will have to manually switch the Help content.

**NAVIGATING DIRECTORIES**

First, a folder is a directory off the root (c:\) or even the root of the hard drive. Sub folders, are contiguous to the root folder and can be nested many sub folders deep.

**FIGURE 7. Folder Tree (from the root)**



Many folders do not show their content unless you ask them to. These folders are protected and only require access when you are troubleshooting or searching for files or sub folders.These folders are:

- Windows - the System Folder
- Program Files - the applications folder
- Recycler - the trash can folder

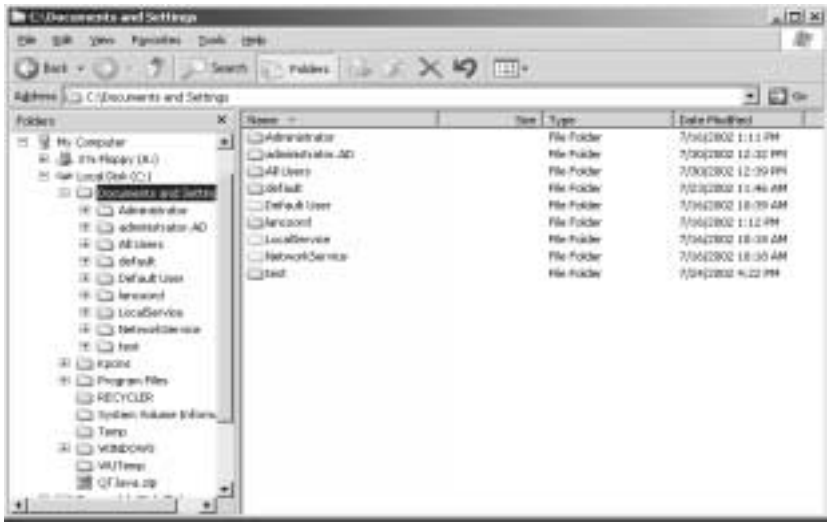
Within the Windows folder there are numerous sub folders that categorize system functionality.

Within the Program Files folder, each application is located in their individual sub folder.

The Recycler folder is hidden and can only be accessed completely through customized folder options.

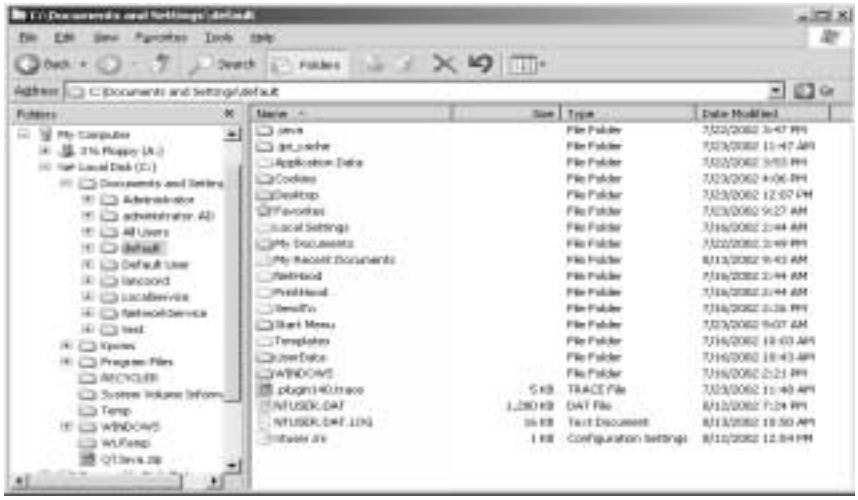
## DOCUMENTS AND SETTINGS

**FIGURE 8. Documents and Settings**



Within the Documents and Settings folder you will find the home folders for all users who have a local user account. All document created on a non-Active Directory workstation will default to their appropriate sub-folder -- designated by the user name as the sub-folder name.

**FIGURE 9. Home Folders**



Within the “home folder” many predefined folders exist including:

- Desktop (those icons located on your desktop)
- My Documents (where all your data goes (aka My Documents on your desktop))
- Start Menu (custom applications only associated with your profile)

As you can see, the home folder contains all of the personalized information regarding a local user.

**SUMMARY**

XP's file system is fairly common to what you'd expect in Windows 2000. The system folder name was changed to Windows (in Windows 2000 and NYT it was WINNT). Most of the same functionality is there with some cool additions (firewall and dual IP). Encryption no longer allows the Administrator to access (or fix) broken encryption so the user gets greater security at a price. All in all Windows XP have closed many holes that Windows 2000 contained.