Controlling Access to Files and Folders

On NTFS volumes, you can set file permissions on files and folders that specify which groups and users have access to them, and what level of access is permitted. NTFS file and folder permissions apply both to users working at the computer where the file is stored and to users accessing the file over the network when the file is in a shared folder. With NTFS you can also set share permissions, which operate on shared folders in combination with file and folder permissions. File attributes (read-only, hidden, system) also limit file access. Figure 3.5 shows the permissions listed on the **Security** tab of the **Properties** dialog box.

FAT16 and FAT32 allow you to set file attributes on files but they do not provide file permissions.

The version of NTFS included with Windows 2000 offers an important new feature for managing security — inheritable permissions. The **Security** dialog box offers the option to **Allow inheritable permissions from parent to propagate to this file object** which is enabled by default.

This feature significantly reduces the time and I/O work required to change the permissions of many files and subfolders. For example, suppose a user wants to change the permissions on a tree consisting of several thousand files. With Windows NT 4.0, each file and folder needs to be individually changed. However, with Windows 2000, if the subfolders and files inherit permissions, they only need to be set for the top-level folder.

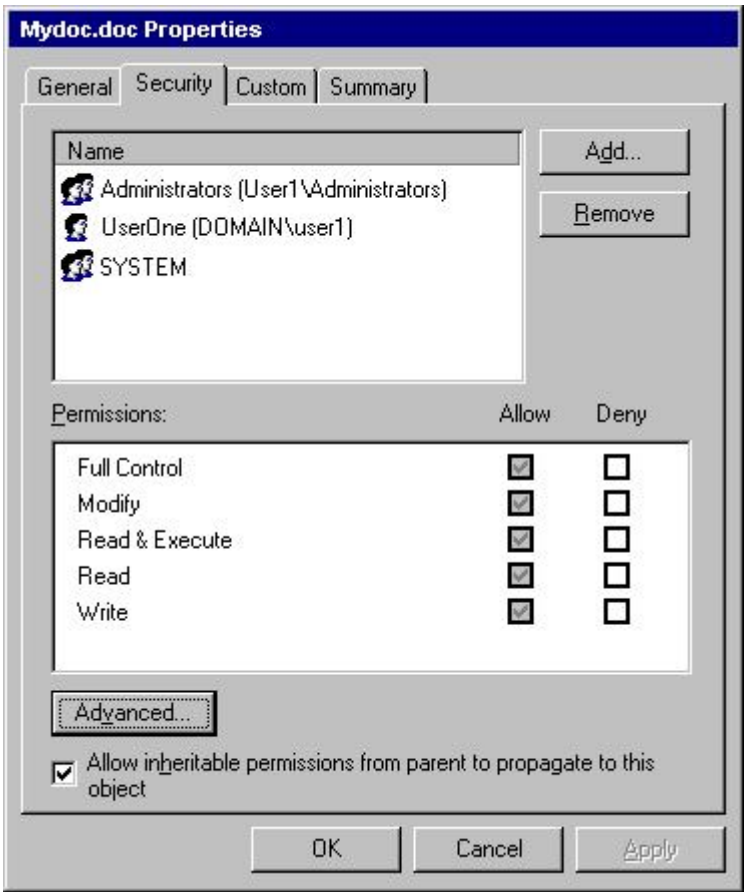

Figure 3.5 Permissions Dialog Box

Figure 3.6 shows the Permissions listed when you select the **Advanced** button on the **Security** tab of the **Properties** dialog box.

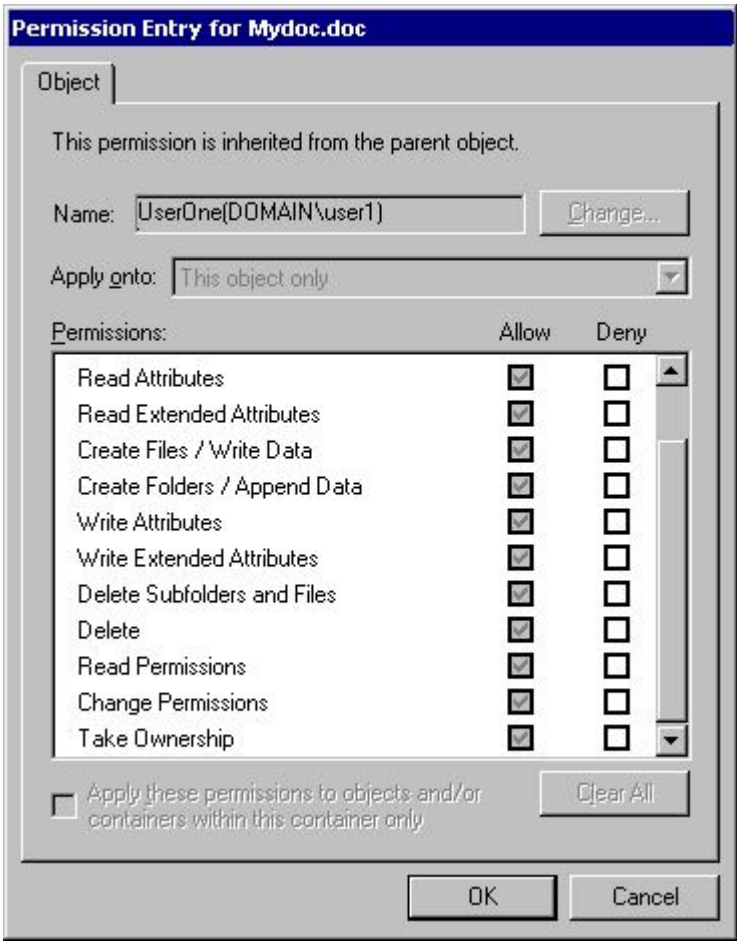

Figure 3.6 Advanced Permissions Dialog Box

Important

To preserve permissions when you copy or move files between NTFS folders, use the Robocopy program on the *Microsoft ® Windows ® 2000 Resource Kit* companion CD.

You can back up and restore data on FAT and NTFS volumes. However, if you back up data from an NTFS volume and then restore it to a FAT volume, you lose security settings and other file information on the restored copies.

You can restore Remote Storage data only to an NTFS volume. For more information about Remote Storage, see "Data and Storage Management" in this book.

Although NTFS provides access controls to individual files and folders, users can perform certain actions on files or folders even if permissions are set on a file or folder to prevent access to users.

For example, you have a folder (Dir1) containing a file (File1), and you grant Full Control to a user for the folder Dir1. If you specify that the user has No Access to File1, the user can still delete File1. This is because the user's Full Control rights in the folder allow the user to delete the contents (files or subfolders) of the folder.

To prevent files from being deleted, you must set permissions on the file itself, and you must set permissions for the folder containing the file.

Anyone who has List, Read, or greater permissions in a folder can view file properties on any file in the folder, even if file permissions prevent them from seeing the contents of the file.

Note

In the **Properties** dialog box, you can use the **Security** tab to deny **Full Control** while leaving **Modify** , **Read & Execute** , **Read** , and **Write** in place.

With FAT volumes, you cannot set any permissions on the individual files and folders. The only security available is the

share permissions that are set on the entire share, that affect all files and folders on that share, and that only function over the network. Once a folder is shared, you can protect the shared folder by specifying one set of share permissions for all files and subfolders of the shared folder. Share permissions are set in much the same way file and folder permissions are set in NTFS. But because share permissions apply globally to all files and folders in the share, they are significantly less versatile than the file and folder permissions used for NTFS volumes.

Share permissions apply equally to NTFS and FAT volumes. They are enforced by Windows 2000, not the individual file system. However, when you move or copy a file from an NTFS to a FAT volume, permissions and other attributes unique to NTFS are lost.

Top Of Page