File Security Overview

Windows' file security underwent a major revision in Windows NT 4.0 service pack 3 and saw additional refinements in Windows 2000. Today, Windows Server 2003's file security system is an inheritance-based system that uses discretionary access control lists (DACLs) to control access to files.

Essentially, any given file or folder can have a set of permissions associated with it. Those permissions either grant or deny the ability to perform specific tasks to specific users or groups. For example, you might configure a file so that members of the Domain Users user group can read the file and so that members of the Sales user group can modify the file. By default, Windows assigns permissions only to the root of each drive, and all other files and folders on the drive inherit that default permission. However, you can turn off inheritance and assign unique permissions to any file or folder. To do so, simply right-click the file or folder and select **Security** from the pop-up menu.

A user's effective permissions on a file are the combination of all permissions assigned to the user's account and any groups to which the user belongs. For example, suppose you have a user account named Joe and that Joe belongs to a group named Sales and a group named Marketing. Now imagine that you assign the following permissions to a file:

- Allow Joe to read the file.
- Allow the Sales group to modify the file.
- Allow the Marketing group to change permissions on the file.

Joe's effective permissions include the permissions for his own account as well as the groups to which he belongs, so he'll be able to read and modify the file, as well as change permissions on the file.

Windows file security also includes the capability to deny permissions. When figuring a user's effective permissions, any Deny entries on the DACL override any Allow entries. Continuing with the example of Joe, suppose you assign the following permissions to a file:

- Joe's permissions: Allow reading.
- Sales group's permissions: Deny reading.
- Marketing group's permissions: Allow reading and writing.

Joe's effective permissions are to write the file. Although both Joe and the Marketing group are allowed to read the file, the Sales group is denied the ability to read the file. That denial overrides all other permissions. Incidentally, although Joe technically has permission to write the file, it's unlikely that he'll actually be able to modify it. That's because most applications, such as Microsoft Word, have to open a file and read it before they can make changes to it.

You can learn more about Windows Server 2003's file security system in the online Help and Support Center, included on Windows Server 2003's Start menu.