

- » The ACL identifies which users and groups can access the object and specifies what level of access each user or group has. A folder's ACL may specify that one group of users can read files in the folder, whereas another group can read and write files in the folder, and a third group is denied access to the folder.
- » Container objects — files and volumes — allow their ACLs to be inherited by the objects that they contain. As a result, if you specify permissions for a folder, those permissions extend to the files and child folders that appear within it.

Table 13-1 lists the six permissions that can be applied to files and folders on an NTFS volume.

TABLE 13-1 File and Folder Permissions

Permission	Description
Full Control	The user has unrestricted access to the file or folder.
Modify	The user can change the file or folder's contents, delete the file or folder, read the file or folder, or change the attributes of the file or folder. For a folder, this permission allows you to create new files or subfolders within the folder.
Read & Execute	For a file, this permission grants the right to read or execute the file. For a folder, this permission grants the right to list the contents of the folder or to read or execute any of the files in the folder.
List Folder Contents	This permission applies only to folders; it grants the right to list the contents of the folder.
Read	This permission grants the right to read the contents of a file or folder.
Write	This permission grants the right to change the contents of a file or its attributes. For a folder, this permission grants the right to create new files and subfolders within the folder.

Actually, the six file and folder permissions comprise various combinations of special permissions that grant more detailed access to files or folders. Table 13-2 lists the special permissions that apply to each of the six file and folder permissions.



TIP

Assign permissions to groups rather than to individual users. That way, if a particular user needs access to a particular resource, add that user to a group that has permission to use the resource.