Setting Access Control Lists

Configuring Access Control Lists

Security within Windows Server 2003 and the NTFS file system is based on a system of access control lists (ACLs). These enable you to enable or disable specific abilities to specific users or groups. You could, for example, provide access to everybody in the Marketing group, as well as Mark Thomas from Sales. You can do this without creating a special group and without providing access to users who do not need access to the folder.

The system uses discretionary access control—users or groups listed are either allowed or denied a particular permission, with the results becoming cumulative. For example, if Mark were a member of the Sales group and you gave Sales specific Read access and listed Mark denying him Read access, Mark would be the only member of the Sales group not able to read the file.

Note that these access control lists are configured on the folder that is being Web published—the information is not separately stored or processed by IIS. Instead, IIS uses the credentials of the user who has authenticated with the system—including through anonymous authentication—and then attempts to access the files and folders using those credentials.

If the underlying filesystem ACLs enable access to the credentials, the information is returned. If the ACLs do not explicitly provide access to the information, access to the object is rejected.

Although this can be confusing—because you have to modify the filesystem to help set Web-based security—in the long run, it makes the process easier. In short, IIS is responsible for authenticating the user and verifying his credentials, and the filesystem is responsible for providing access to the information based on those credentials.

The different permissions that you can apply to users and groups within a file system are as follows:

Permission	Folder Effect	File Effect
Read	Permits viewing the names of files/folders within the folder.	Permits viewing of the file.
Write	Permits the addition of files or subfolders to the folder.	Permits writing to the file.
Read & Execute	Permits viewing names of files/folders within the folder and executing applications/scripts within it.	Permits viewing the contents and executing the file.
List Folder Contents	Permits viewing the names of files/folders within the folder.	N/A
Modify	Permits reading and writing to the list of files/folders within the folder, and deleting the folder.	Permits reading, writing, and deleting of the file.
Full Control	Permits read/write access to the folder contents list, deletion of the folder, and the deletion of contained files and folders.	Permits reading, writing, and deleting of the file.

To set the ACL for a file or directory

1. Use Explorer to locate the file or directory that you want to adjust permissions for.
2. Right-click on the directory and select Properties.
3. Click Security to change to the security panel.
4. To add a new access control setting to the directory, click Add. You will be asked to select the users or groups who this access control setting will be applied to. Enter the names you want to add and click OK—remember to prefix any domains outside the server's current default domain. The system will check that the names are valid within the current domain scope.
5. Select the group or user who you want to adjust the permissions for. Select the appropriate permissions and whether you want to allow or deny access accordingly. Note that if you leave a permission blank, its value is inherited from any appropriate group.
6. To remove an access control setting, click Remove.
7. Click OK to accept the settings. Click Cancel to cancel any changes you have made. Click Apply to apply the changes without closing the properties window.