Use Access Control to Restrict Who Can Use Files

Published: August 24, 2001
The NTFS file system available in Windows XP offers several security advantages not available in previous versions of Windows without NTFS. One such advantage is access control. You can restrict who has access to data on your computer, or on the network, using access control lists in Windows XP on a drive formatted to use NTFS. The access control features allow you to restrict access to a specific user, a computer, or a group of users.

Setting Permissions on Files and Folders

You set permissions to define the type of access granted to a user or group. For example, you can grant Read and Write permissions to the entire Finance group for the file *payroll.dat*. When you set up permissions, you specify the level of access for groups and users. For example, you can let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file. You can set similar permissions on printers so that certain users can configure the printer and other users can only print from it. To change permissions on a file or folder, you must be the owner of that file or folder, or you must have permission to make such changes.

Top of page

Group Permissions

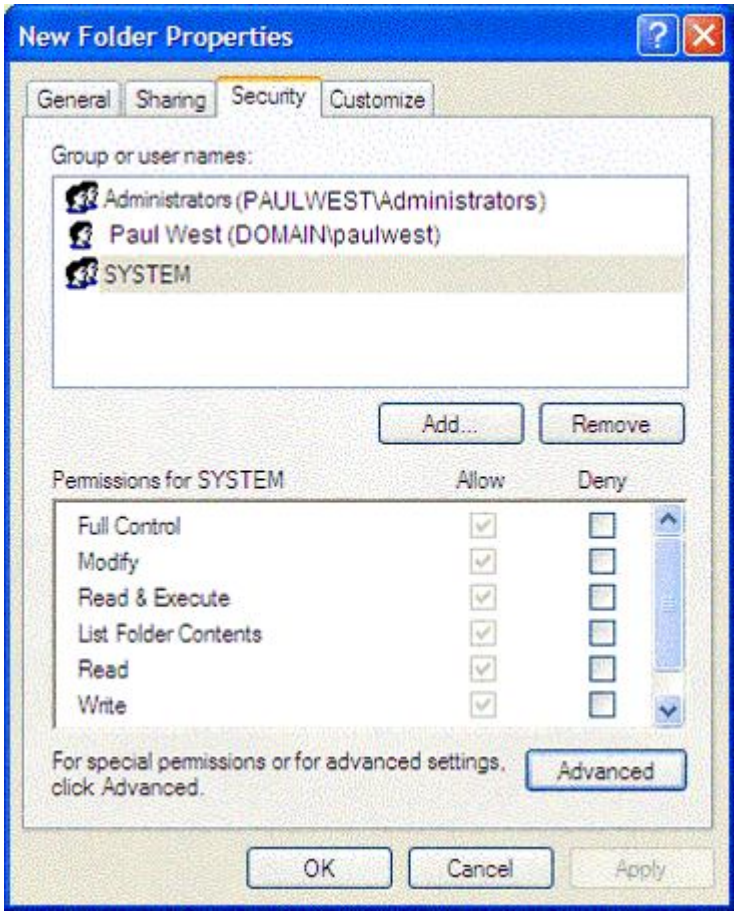
For best results, assign permissions to groups rather than to users, this saves you from maintaining access control for each user; assign **Full control**, if appropriate, rather than individual permissions. Use **Deny** to exclude a subset of a group which has Allowed permissions, or to exclude one special permission when you have already granted full control to a user or group.

The type of permissions you can grant depend on the type of object. For example, the permissions for a file are different from those for a registry key. However, some permissions are common, including:

- Read permissions
- Modify permissions
- Change owner
- Delete

To set, view, change, or remove file and folder permissions

1. Open Windows Explorer. (Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Windows Explorer**.)
2. Locate the file or folder for which you want to set permissions.



3. Right–click the file or folder, click **Properties**, and then click the **Security** tab. (If you do not see the **Security** tab, you may not be joined to a domain. See **To display the Security tab** below.)

4. Do one of the following:

    - To set permissions for a group or user that does not appear in the **Group or user names** box, click **Add**. Type the name of the group or user you want to set permissions for and then click **OK**. (When adding a new user or group, by default, this user or group will have **Read & Execute**, **List Folder Contents**, and **Read** permissions.)

    - To change or remove permissions from an existing group or user, click the name of the group or user.

5. Do one of the following:

    - To allow or deny a permission, in the **Permissions for *User or Group*** box, select the **Allow** or **Deny** check box.

    - To remove the group or user from the **Group or user names** box, click **Remove**.

6. If the check boxes under **Permissions for *user or group*** are shaded or if the **Remove** button is unavailable, then the file or folder has inherited permissions from the parent folder.

To display the Security tab

- Open Folder Options in Control Panel. (Click **Start**, click **Control Panel**, click **Appearance and Themes**, and then click **Folder Options**.)

- On the **View** tab, under **Advanced settings**, clear **Use simple file sharing [Recommended]**.

Top of page
Related Links

- How-to Article: Encrypt Your Data to Keep It Safe

- Technical Overview: What's New in Security for Windows XP

Top of page