ITFreeTraining

NTFS Allow and Deny
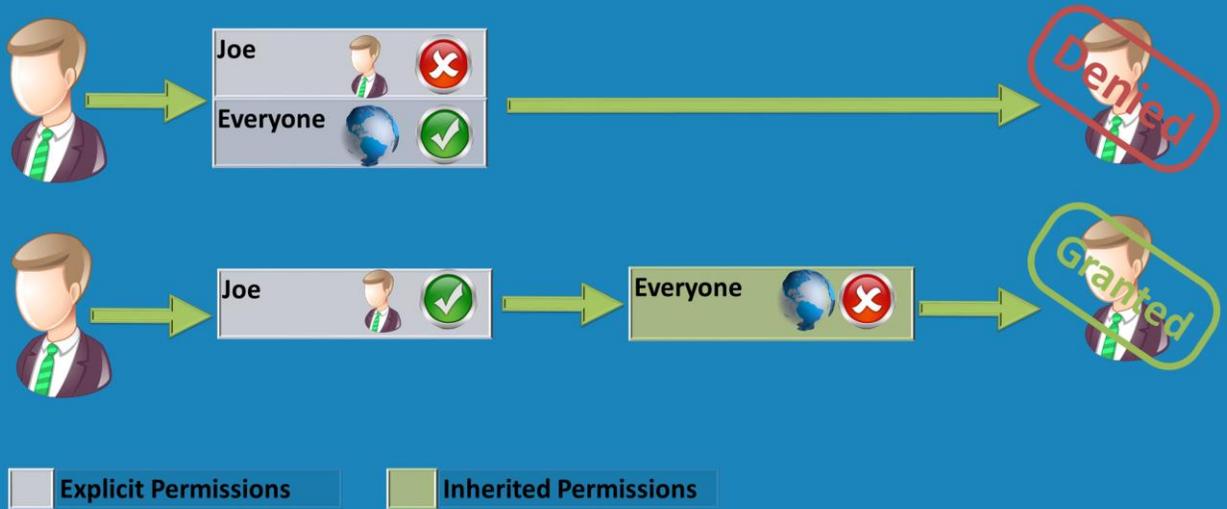
For the free video please see
http://itfreetraining.com/server#ntfs-deny

NTFS Deny Permission

The deny permission prevents user access. This video will look at how to use the deny permission and the potential pitfalls of the deny permission the administrator should be aware of before using it.

Allow and Deny

The deny permission in most cases will deny the user access. In some cases when explicit and inherited permissions are combined, the deny permission will not work. Deny permissions are always sorted to the top of the NTFS permission list and thus read first. In this example, if you have explicit permissions configured that allow access and inherited permissions that deny access the user will still have access. This is because of the order that permissions are checked in.

Deny permissions are always sorted to the top of the NTFS explicit or inherited permission list and thus checked first. However, explicit permissions are checked first. If there is a match allowing access, the user is allowed access. The next check is to check the inherited permission. If there is a match here the user is allowed access. You can see that if there is an allow access in the explicit permission, the inherited permissions will never be checked. For this reason, if there is a deny permission in the inherited permission and an allow permission in the explicit permission, the inherited permissions will never be checked and thus the deny permission will never be used.

Allow and deny

- Denies sorted to the top
- Explicit processed first and then inherited

Checked First   **Checked Second**

Joe	❌
Everyone	✅
Sales Group	✅

Domain Users	❌
Jane	✅
Marketing Group	✅

☐ **Explicit Permissions**   ☐ **Inherited Permissions**

Demonstration

This demonstration will look at how an inherited deny permission will be ignored if an allow permission has been explicitly configured.

1) Right click on the folder Joe and select the option properties.

2) In the properties for the folder select the tab security.

3) Click the button edit.

4) From the security window press the button add.

5) In this case the everyone permission will be added and the only permission that will be configured for it is the deny write access. A warning dialog will appear stating deny permission will override other permissions.

6) Once the permissions have been configured, if a new file or folder is attempted to be created in the folder or any sub folder, an error message will appear stating that access has been denied.

7) The next step is to right click on a sub folder and select properties and then select the security tab. On the security tab press the button edit. The permission that will be added will be domain users with write permission. This means the sub folder will have everyone deny write permission from inheritance and domain users allow write explicit permission.

8) With these permissions configured, the user will still be able to create files and folders in the sub folder. This is because the explicit permissions are checked first and since the user is a member of the domain users group, they will be allowed access. The deny permission that is inherited is never checked because there is a match under explicit permissions.

9) Also notice that you are not able to change inherited permissions once they are configured, however you can tick options that are not already ticked. For example, if the deny permission is ticked via inheritance, you can tick the allow tickbox and override the inheritance allowing access.

When configuring deny permissions, you should also consider that often a domain administrator will be a member of the domain users group. If you deny the domain users, you may also deny the administrator from having access as well.

Multiple groups

When a user is a member of multiple groups, this can cause problems when the deny permission is used. For example, if Joe is a member of the sales and marketing group, and if the deny permission is used on a file share to deny the sales group access, Joe will be denied access. To get around this, it is better to simply remove the sales group from the access list. This prevents them from accessing the file share since they do not have access and does not prevent users like Joe who are members of multiple groups from accessing the file share. For reasons like these, many administrators will only use the deny permission when there is no other way of achieving the required result.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"Windows 101: Know the basics about NTFS permissions"
http://www.techrepublic.com/article/windows-101-know-the-basics-about-ntfs-permissions