

## Combining Shared Folder and NTFS Permissions

- When you combine NTFS permissions and share permissions the most restrictive effective permission applies.
  - For example, if you share a folder and assign the *share permission* READ to EVERYONE and assign FULL CONTROL *NTFS permissions* to Everyone, users connecting through the network will have Read permissions.
- When accessing a file locally, only NTFS permissions apply

1

## Calculating Effective Permissions

- Both Share and NTFS Permissions are Cumulative
  - Cumulative permissions:
    - Permissions are combined when a user is not explicitly denied access
    - A user's effective permissions for a resource are the sum of the NTFS permissions that you assign to the individual user account and to all of the groups to which the user belongs.
    - i.e. If a user has Read permissions for a folder and is a member of a group with write permissions for the same folder, the user's cumulative permissions are both Read and Write

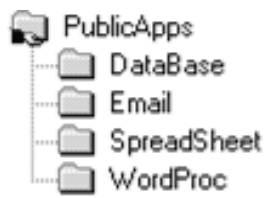
2

## Calculating Effective Permissions

- To calculate effective permissions when combining share permissions and NTFS
  1. Determine the *effective* NTFS permissions
  2. Determine the *effective* share permissions
  3. Take the most restrictive of the two.

3

## Sample Calculation



### Share Permissions of PublicApps

- Everyone Change

### NTFS Permissions of PublicApps

John: Full Control  
Sales: Read

You share a folder on your computer and you assign the share permission Change to Everyone. John, a user from the Sales Department, has been granted Full Control NTFS permissions to the folder. John is a member of the Sales Group, which has been assigned the READ NTFS permission. What are John's effective permissions when connecting to the share from across the network?

4

## Sample Calculation



### Share Permissions of PublicApps

- Everyone Change

### NTFS Permissions of PublicApps

John: Full Control  
Sales: Read

John's Effective NTFS Permissions: Full Control

John's Effective Share Permissions: Change

Most Restrictive of the two: Change

5

## Rules to Remember

- If you or a group you belong to is on both the share permissions access control list (ACL) and the NTFS ACL, you can browse into the share
- If you or a group you belong to is on only the share ACL, you cannot browse in but, if you have rights to folders beneath the shared folder you can access them using a UNC path.
- If you or a group you belong to are only on the NTFS ACL, you cannot browse into the share and you cannot access any folders beneath the share, even if you have rights to them.

6

## A Suggested Security Assignment for PUBLIC APPLICATION FOLDERS

Permissions assigned here assume that all users in the domain should be able to run programs that exist in any of the share's subfolders.



### Share Permissions

- Everyone Full Control

### • NTFS Permissions

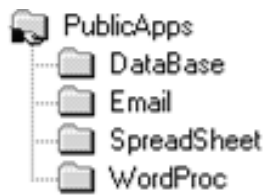
- PublicApps: Administrators Full Control  
Users Read & Execute; List Folder Contents; Read

If the PublicApps folder is created at the root of the drive and Microsoft's default NTFS permissions haven't been changed at the root, you can use the default NTFS permissions.

7

## A Suggested Security Assignment for PUBLIC APPLICATION FOLDERS

Permissions assigned here assume that all users in the domain should be able to run programs that exist in any of the share's subfolders.



### Share Permissions

- Users Read
- Administrators Full Control

### NTFS Permissions

- PublicApps: Administrators Full Control  
Users: Read and Execute  
List Folder Contents  
Read

If the PublicApps folder is created at the root of the drive and Microsoft's default NTFS permissions haven't been changed at the root, you can use the default NTFS permissions.

8

## A Suggested Security Assignment for PUBLIC DATA FOLDERS

Permissions assigned here assume that all users are able to add to, delete from and change the contents of files in the shared folder area. Users should not however be able to change permissions on a file or folder nor should they be able to take ownership of a file or folder.



### Share Permissions

- Everyone Full Control

### NTFS Permissions

- PublicData: Administrators Full Control  
Users everything *but* Full Control

9

## A Suggested Security Assignment for PUBLIC DATA FOLDERS

Permissions assigned here assume that all users are able to add to, delete from and change the contents of files in the shared folder area. Users should not however be able to change permissions on a file or folder nor should they be able to take ownership of a file or folder.



### Share Permissions

- Administrators Full Control
- Users Change

### NTFS Permissions

- PublicData: Administrators Full Control  
Users everything *but* Full Control

10

## A Suggested Security Assignment for PRIVATE APPLICATION FOLDERS

Permissions assigned here assume that users in each department should only have access to their department's applications. (i.e., Accounting can only access Accounting; Sales can only access Sales, etc.)



### Share Permissions

Everyone Full Control

- **NTFS Permissions**
- PrivateApps: Administrators Full Control
  - Remove Inheritance from above (do not allow inheritable permissions from this object's parent) After removing the inheritance make sure Administrators have full control applied to This folder, subfolders and files.
- Each subfolder
  - Administrators should already be assigned full control because of inheritance
  - Assign each group the following permissions to their department's respective folder (i.e., Sales group to the Sales folder; Marketing group to the Marketing folder, etc.) (users in each department will have to access their respective folder via the UNC path)
    - Read and Execute,
    - List Folder Contents
    - Read

11

## A Suggested Security Assignment for PRIVATE APPLICATION FOLDERS

Permissions assigned here assume that users in each department should only have access to their department's applications. (i.e., Accounting can only access Accounting; Sales can only access Sales, etc.)



### Share Permissions

Everyone Full Control

- **NTFS Permissions**
- PrivateApps: Administrators Full Control
  - Users Read and Execute, List Folder Contents, Read
  - If the PrivateApps folder is created at the root of the drive and Microsoft's default NTFS permissions haven't been changed at the root, you can use the default NTFS permissions.
- Each subfolder
  - Remove Inheritance from above (do not allow inheritable permissions from this object's parent) After removing the inheritance make sure Administrators have full control applied to This folder, subfolders and files.
  - Assign each group the following permissions to their department's respective folder (i.e., Sales group to the Sales folder; Marketing group to the Marketing folder, etc.)
    - Read and Execute,
    - List Folder Contents
    - Read

12

## A Suggested Security Assignment for PRIVATE DATA FOLDERS

Permissions assigned here assume that users in each department should only have access to their department's data. Users in each department should be able to add to, delete from and change the contents of files in their department's folder.



### Share Permissions

- Everyone Full Control

### NTFS Permissions

- PrivateData: Administrators Full Control
  - Remove Inheritance from above (do not allow inheritable permissions from this object's parent) After removing the inheritance make sure Administrators have full control applied to This folder, subfolders and files.
- Each subfolder
  - Administrators should already be assigned full control because of inheritance
  - Assign each group everything *but* Full Control to their respective folder (i.e., Sales group to the Sales folder; Marketing group to the Marketing folder, etc.) (users in each department will have to access their respective folder via the UNC path)

13

## A Suggested Security Assignment for PRIVATE DATA FOLDERS

Permissions assigned here assume that users in each department should only have access to their department's data. Users in each department should be able to add to, delete from and change the contents of files in their department's folder.



### Share Permissions

- Everyone Full Control

### NTFS Permissions

- PrivateData: Administrators Full Control  
Users Read and Execute, List Folder Contents, Read
  - If the PrivateData folder is created at the root of the drive and Microsoft's default NTFS permissions haven't been changed at the root, you can use the default NTFS permissions.
- Each subfolder
  - Remove Inheritance from above (do not allow inheritable permissions from this object's parent) After removing the inheritance make sure Administrators have full control applied to This folder, subfolders and files.
  - Assign each group everything *but* Full Control to their department's respective folder (i.e., Sales group to the Sales folder; Marketing group to the Marketing folder, etc.)

14