Server Administration

Module Number: 03

Module Name: Configuring File and Share Access Permissions

Version Code:SA1_Updated
Released Date:30-Jan-2019

Configuring File and Share Access Permissions

AIM:

Explores the file configurations, file share and different access permissions.

Configuring File and Share Access Permissions

Objectives:

The Objectives of this module is:

- To understand the file sharing strategies, arranging shares, access controlling.
- To understand the drive mapping, folder share, assigning permissions.
- To understand the windows Permission Architecture and Basic.
- To get the permissions and file server resource manager.
- To understand the file screening, file groups and file resource management.

Configuring File and Share Access Permissions

Outcomes:

At the end of this module, you are expected to:

- Elaborate the different types of windows file sharing strategies and mapping of drives.
- Explain Windows permission architecture and basics.
- Install the File Server Resource Manager.
- Explain the different types of permissions and its working.
- Explain the functionality of file screening and storage report management.

Configuring File and Share Access Permissions

Contents

1. Designing a File-Sharing Strategy
2. Arranging shares, controlling access and mapping drives
3. Creating Folder Shares, Assigning Permissions, Understanding the windows Permission Architecture and Basic
4. Advanced Permissions, Allowing and Denying Permissions, Inheriting Permissions.
5. Understanding Effective Access, Setting Share Permissions, Understanding NTFS Authorization, Assigning Basic NTFS Permissions
6. Understanding Resource Ownership, Combining Share and NTFS Permissions, Installing File Server Resource Manager
7. Using, creating, changing Quotas, Managing Files with File Screening, Creating File Groups, Creating a File Screen, Creating a File Screen Exception
8. Creating a File screen Template. Storage Reports Management

Designing a File-Sharing Strategy

Designing a File-Sharing Strategy

- File sharing is the public or private sharing of computer data or space in a network with various levels of access privilege.
- While files can easily be shared outside a network (**for example**, simply by handing or mailing someone your file on a diskette), the term file sharing almost always means sharing files in a network, even if in a small local area network.
- File sharing has been a feature of mainframe and multi-user computer systems for many years. With the advent of the Internet, a file transfer system called the File Transfer Protocol (FTP) has become widely used.

Designing a File-Sharing Strategy

- Among the best-known network file systems is not surprisingly the Network File System (NFS). Originally developed by Sun Microsystems for its UNIX-based systems, let you read and, assuming you have permission, write to sharable files as though they were on your own personal computer.
- Files can also be shared in file systems distributed over different points in a network. File sharing is involved in groupware and a number of other types of applications.
- Some basic strategies should be kept in mind while file sharing is as follows:

Designing a File-Sharing Strategy

1. Develop Standard Permissions.
2. Keep the Permissions Simple.
3. Use Security Groups.
4. Give Groups Succinct and Intuitive Names.
5. Define Permissions Sets that Reflect Department or Job.
6. Know How to Determine Effective Permissions.
7. Do not Use the Everyone Group.
8. Avoid Folder Spread.
9. Create a Global Deny Group.
10. Give Users Centrally Managed Shortcuts to Shared Resources.

Arranging Shares, Controlling Access and Mapping Drives

Configuring File and Share Access Permissions

Arranging Shares

- Further complicating the storage issue is the need for many businesses to share documents between employees. Within an office, this is typically accomplished by using a file server or network attached storage device (NAS).
- **Example,** If shared mobile access is required, documents can be stored in the cloud and shared by assigning access permissions.
- Proper organization of digital documents is especially critical in a shared environment - if one of your employees is absent (temporarily or permanently!) you should be able to easily locate any documents created or managed by that person.

Arranging Shares

Some file management tips will help you keep your files accessible:

1. Use the default installation folders for program files.
2. One place for all documents.
3. Create folders in a logical hierarchy.
4. Nest folders within folders.
5. Follow the file naming conventions.
6. Be specific.
7. File as you go.
8. Order your files for your convenience.
9. Cull your files regularly.
10. Back up your files regularly.

Configuring File and Share Access Permissions

Controlling Access

- You can share files on your computer with other users over the network, and despite this might seem complicated, it's actually a simple task when using the tools the operating system provides.
- Depending on your network environment and what you're trying to accomplish there are at least four ways to set up file sharing

1. You can use Public folder, which is a special setup that allows sharing files over the local network without configuring permissions.
2. You can share content using the File Sharing feature. Then there is a Homegroup, which unlike Public folder, this option automatically shares your libraries folders (Pictures, Videos, Music, Documents), Printers, and other devices connected to your PC.

Configuring File and Share Access Permissions

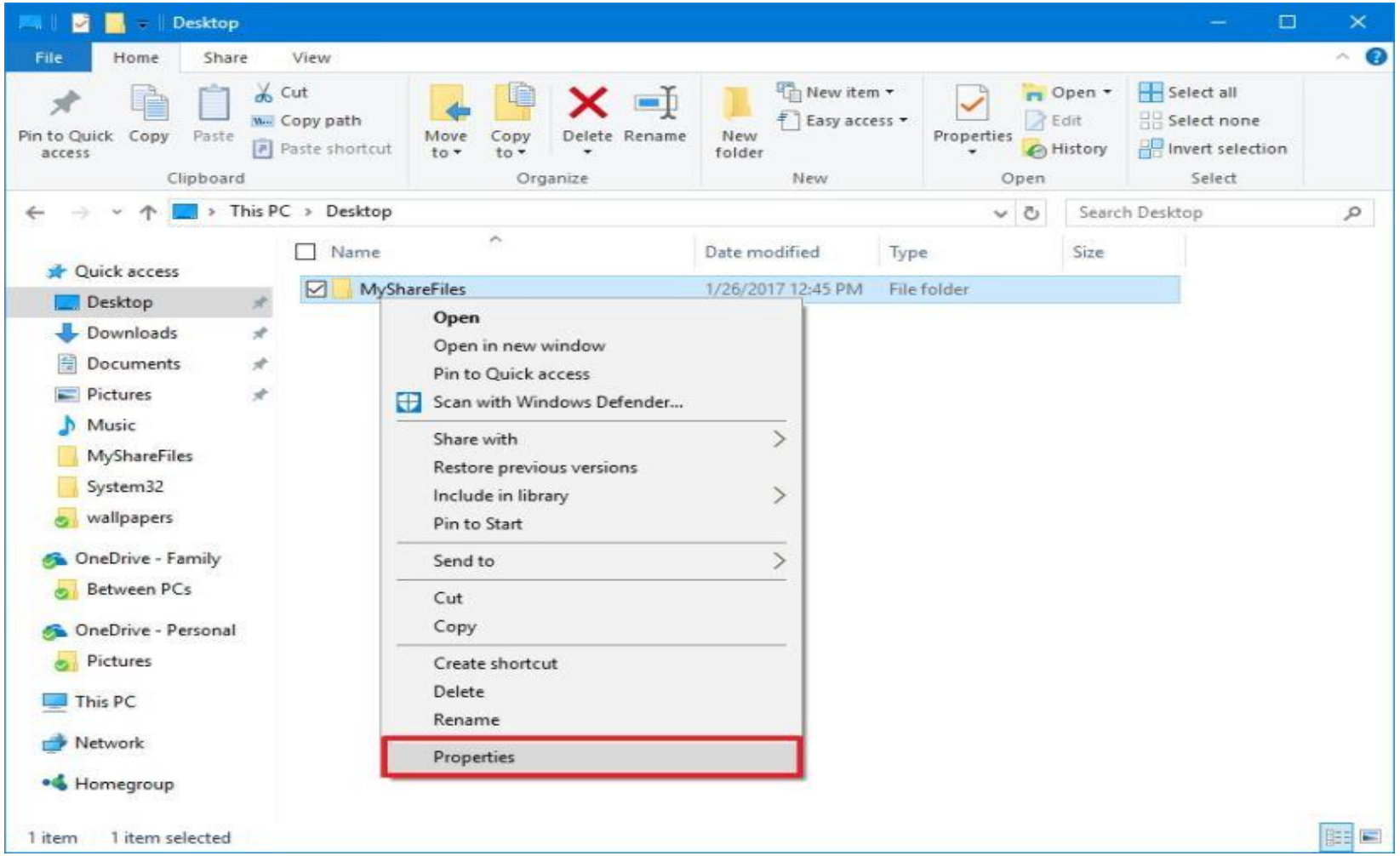
Controlling Access

- If you are looking to share files with other people across the internet, you can use file sharing on OneDrive.
- There are two ways to share files using File Explorer: you can use the basic settings, which allows you to quickly share files on the network with minimal configuration, or you can use the advanced settings to set custom permissions and set other advanced options.
- **Sharing files using basic settings**

1. Open-File Explorer.
2. Navigate to the folder you want to share.
3. Right-click the item, and select Properties.

Configuring File and Share Access Permissions

Controlling Access

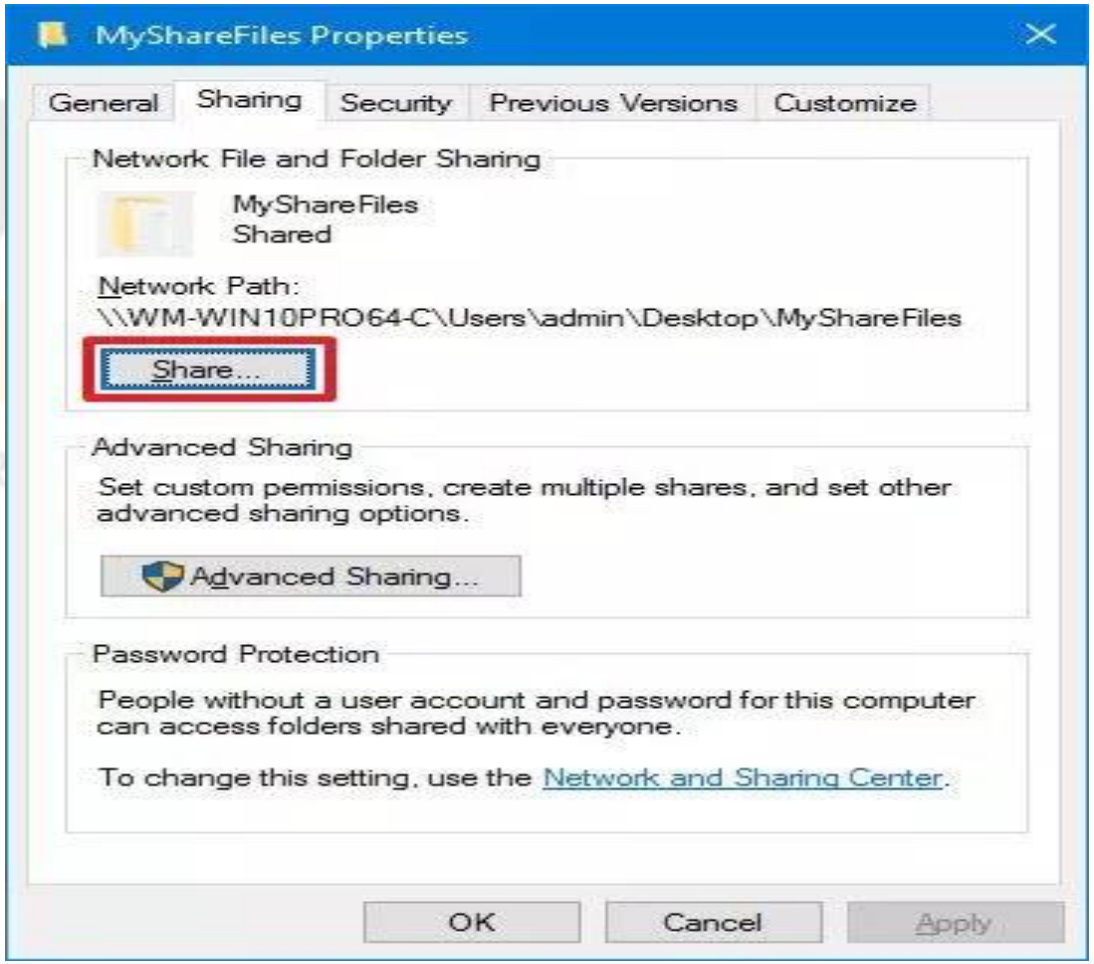


Configuring File and Share Access Permissions

Controlling Access

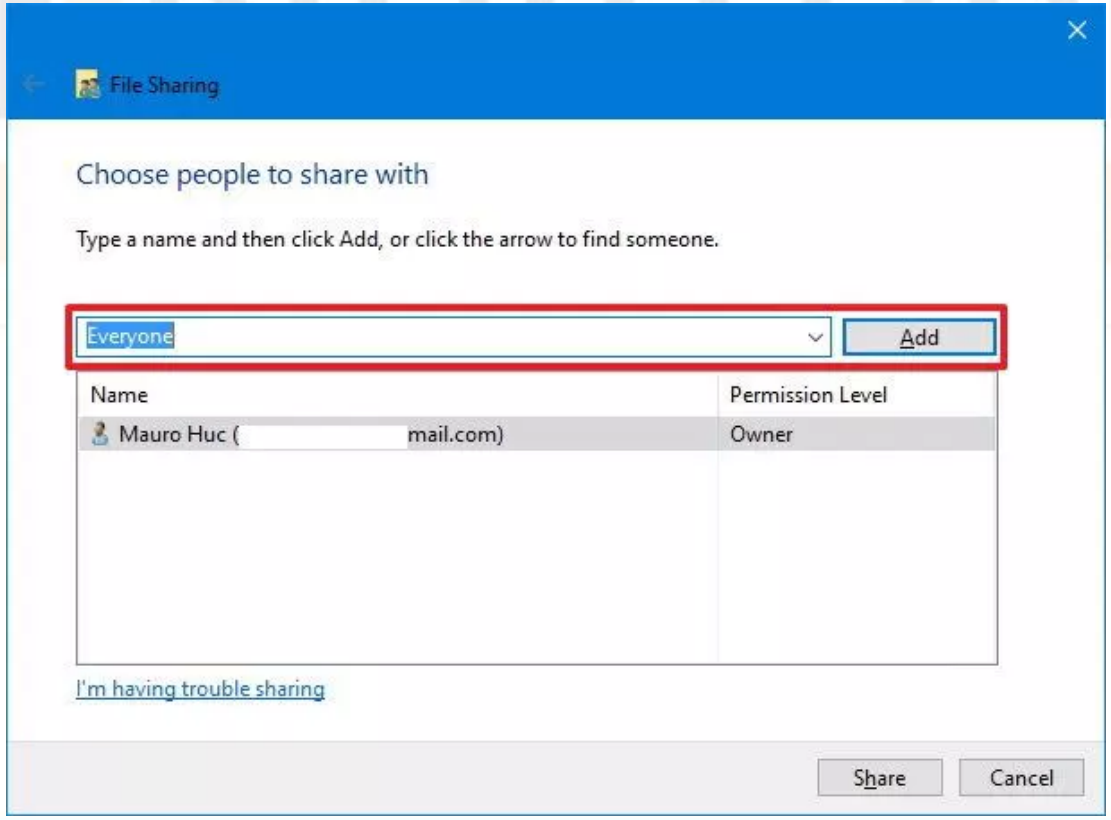
4. On the Properties window, click the Sharing tab.

5. Click the Share button.



Controlling Access

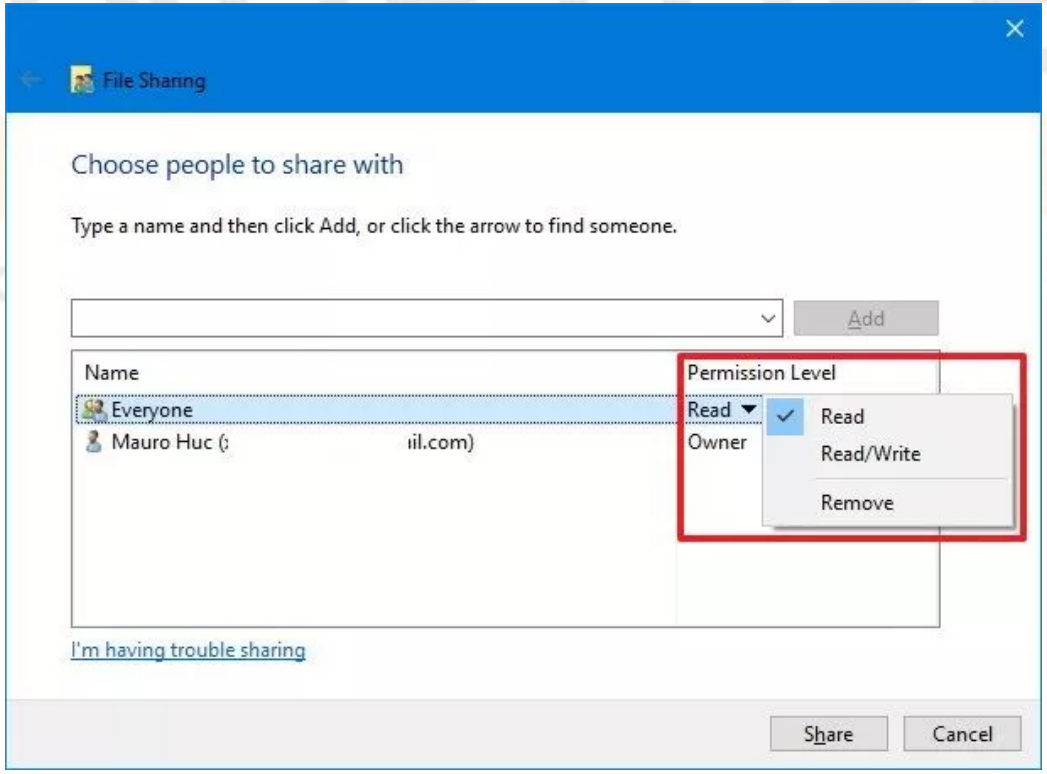
6. Use the drop-down menu to select the user or group to share file or folder. For the purpose of this guide, select the Everyone group. Click the Add button.



Configuring File and Share Access Permissions

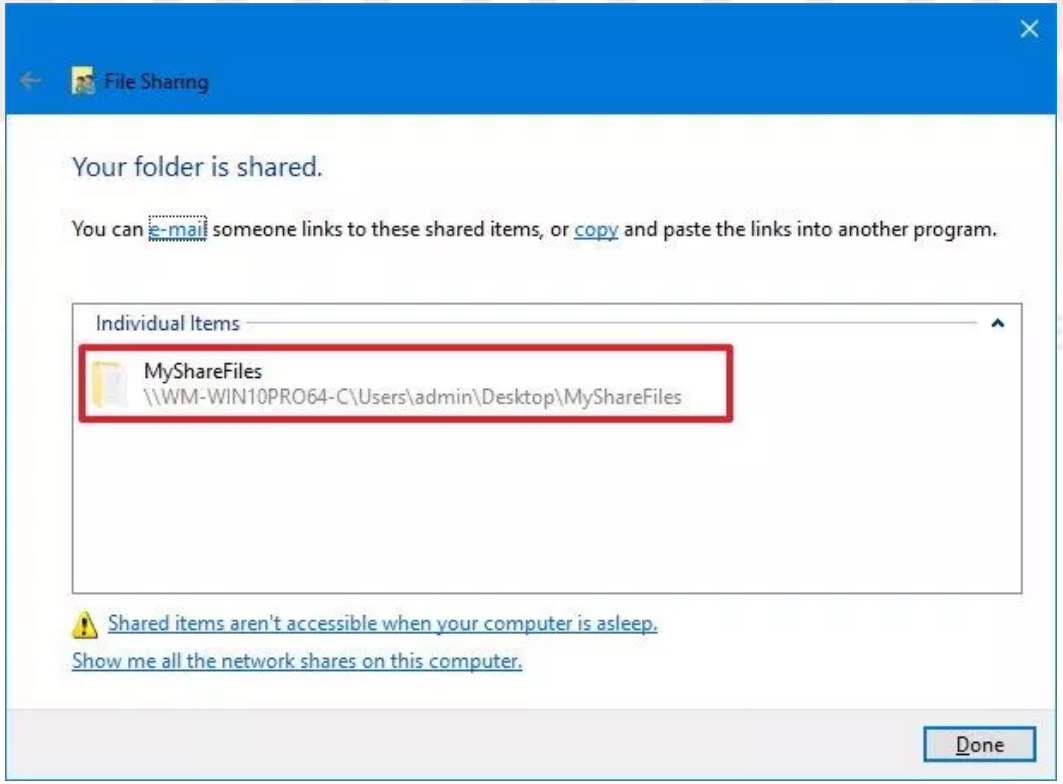
Controlling Access

7. Under Permission Level, select the type of sharing permissions you want the folder to have. For example, you can select Read (default) if you only want users to be able to view and open files. If you select Read/Write, users can view, open, modify, and delete the content on the folder you're sharing. Click the Share button.



Controlling Access

8. Note the network path for the folder that other users will need to access the content over the network and click Done. Click Close to complete the task.



Controlling Access

- **Sharing files using advanced settings**

To share files on your local network using the advanced sharing settings, do the following:

1. Open-File Explorer.
2. Navigate to the folder you want to share.
3. Right-click the item, and select Properties.
4. On the Properties window, click the Sharing tab.
5. Click the Advanced Sharing button.
6. Check the Share this folder option.
7. If you want users to be able to edit the files, delete, and create new documents in the location, you'll need to click the Permissions button.

Controlling Access

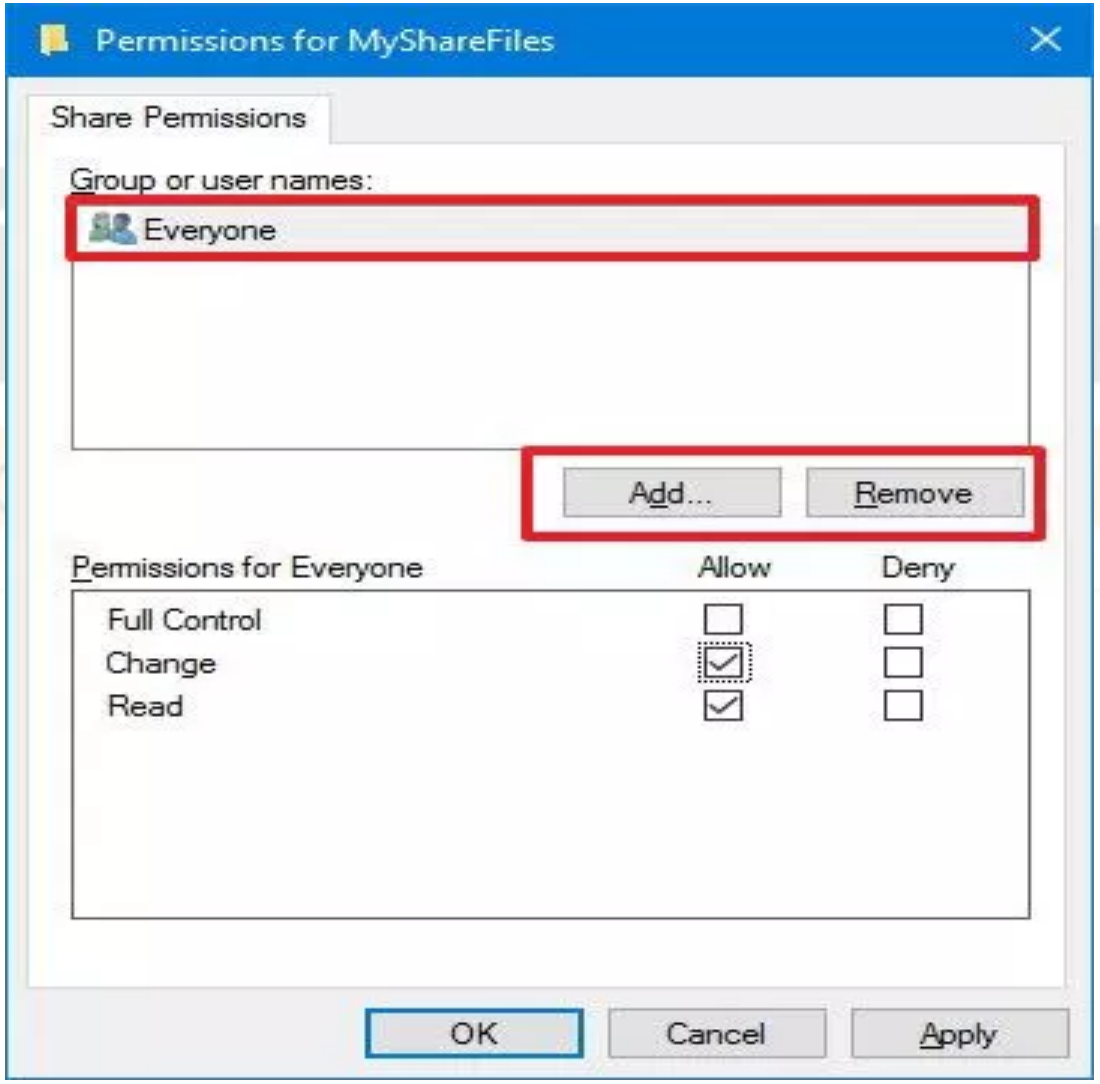
8. On the Permissions window, you'll notice the Everyone group is the default option highlighted. In the section below, you can customize the permissions for a specific user or group. If you want users to be able to open, edit, delete, and create files, then make sure to check the Read and Change permissions under Allow.
9. Click Apply. Click OK.

Click OK again to complete the task.

- **Sharing files with a specific user**
    1. Select the Everyone group and click the Remove button.
    2. Click the Add button.

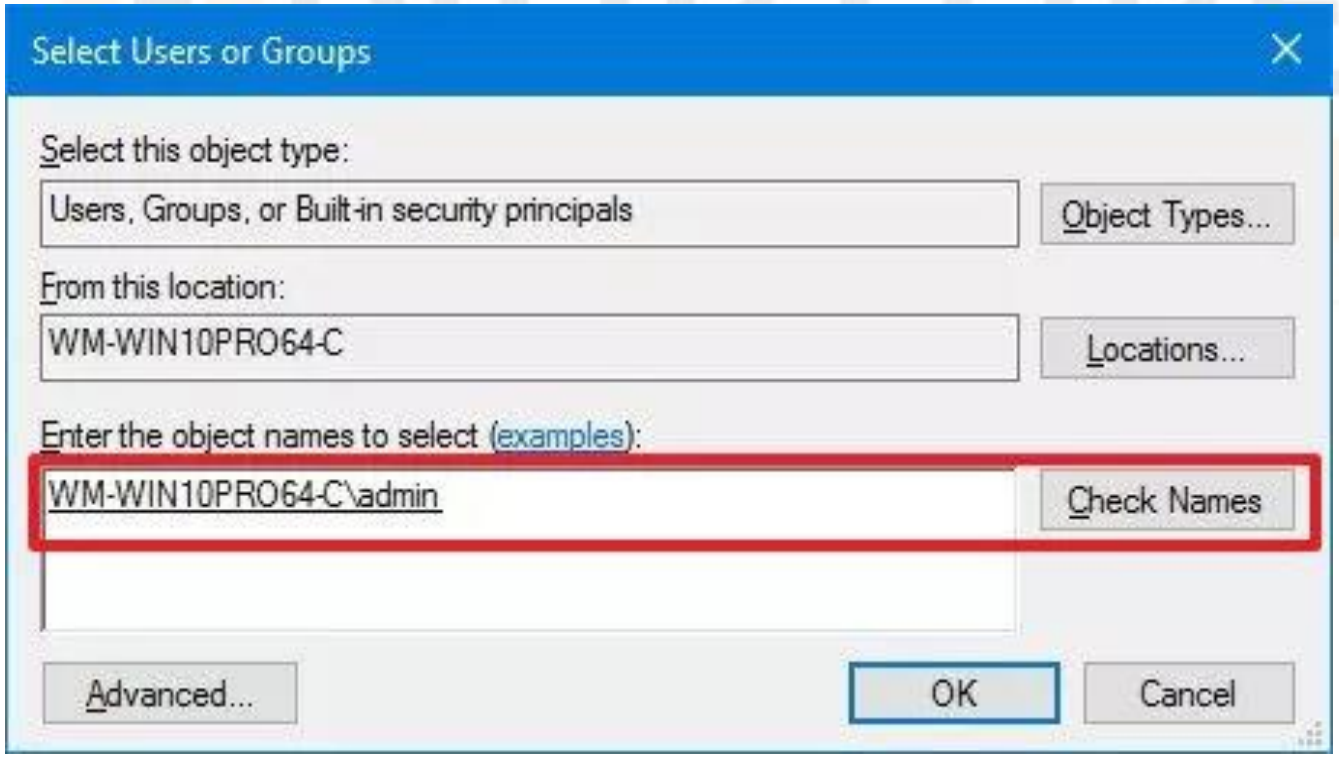
Configuring File and Share Access Permissions

Controlling Access



Controlling Access

3. Type the name of the user you want to share the files.
4. Click the Check Name button. Click OK.



Controlling Access

5. Select the user account, and you'll notice that the Read permission is checked by default. If you want the user to be able to edit, delete, and create new files, make sure to also check the Change permission option. Click Apply. Click OK.

Once you completed the steps, the shared content should be available when browsing the remote computer on File Explorer > Network.

Configuring File and Share Access Permissions

Mapping Drives

- If you have access to multiple computers on a network, big or small, connecting to these resources can be critical to your productivity. For instance, in a large enterprise environment, users are often required and recommended to save data to a Mapped Network drive so co-workers can access the files. A network drive is usually a shared folder or computer that is available on a network and makes it easy to access using File Explorer just like a normal hard disk.
- This is done, so everyone has consistent access to resources no matter the device or location. Admins can also regulate who has access to directories in a network share to keep data safe. Even if you are not in a complex network environment (your home network), you can also use Mapped Network drives to store, access, and retrieve data on another computer, home server, or a Network Attached Storage (NAS) device.

Mapping Drives

Map a Network Drive in Windows 10

- Launch File Explorer on the Taskbar or Start menu, and select This PC (formerly My Computer) in the Navigation Pane.
- Next select Map Network Drive under Computer tab on the Ribbon.
- This will launch the Map Network Drive wizard. Here you will see a list of options, which includes assigning an available drive letter. You can then type the path, to the Network Share or you can browse to it.
- Make sure to check the box *Reconnect at a sign on* so it will always be accessible when you sign in and then click Finish.
- The Mapped Network Drive will then appear in This PC as a Network Location. If the drive is not available, you will see an X emblem on the icon. If at any time you want to remove it, just right-click the icon and click Disconnect.

Mapping Drives

Kerberos and Mapped Drives

- In a Win2K domain, the Kerberos authentication functions determine whether you can access shares. Kerberos relies on the Windows Time Service during authentication, and if the local computers' clock does not show the same time (within a certain tolerance) as the remote computers' clock, Kerberos would not let you access shares on the remote computer.
- The default behaviour of a Win2K computer in a Win2K domain is to sync its time with the DC's time every 45 minutes. When the clock times match, the synchronisation interval is incrementally extended until it reaches 8 hours or until the clocks do not match.

Mapping Drives

You can easily create a shortcut to another drive or folder shared on your network by mapping that location.

1. **Open-File Explorer and select This PC.**
2. **Click the Map network drive button** in the ribbon menu at the top, then **select "Map network drive."** (This is under the Computer tab, which should open automatically when you go to This PC, as above).
3. **Select the drive letter you want** to use for the network folder, then **hit Browse.**
4. **Navigate to the folder** you want to map and **hit OK** after selecting it.

Mapping Drives

5. **Confirm your selection** and **click Finish.** You can choose to reconnect to the folder every time you sign in so it is always available to you and, if needed, use a different user account to connect to the folder.

   - When you are done, you should see the new drive letter under This PC and will be able to access its contents like you would any other folder. If you want to disconnect the network drive, right-click on it and select "Disconnect".

Creating Folder Shares, Assigning Permissions, Understanding the windows Permission Architecture and Basic.

Creating Folder Shares

- The following procedures explain how to create a shared folder on a computer running Windows, and how to confirm the computer's information. In these examples, Windows XP Professional is the operating system, and the computer is a member of a network domain.
- **Step 1: Creating a shared folder on a computer running Microsoft Windows**
- Create a shared destination folder in Windows and enable sharing.
- You must log in as an Administrators group member to create a shared folder.
- If "Everyone" is left selected in step 5, the created shared folder will be accessible by all users. This is a security risk, so we recommend that you give access rights only to specific users. Use the following procedure to remove "Everyone" and specify user access rights.

Creating Folder Shares

- Create a folder, just as you would create a normal folder, in a location of your choice on the computer.
- Right-click the folder, and then click [Sharing and Security].
- On the [Sharing] tab, select [Share this folder].
- Click [Permissions].
- In the [Group or user names:] list, select "Everyone", and then click [Remove].
- Click [Add].
- In the [Select Users or Groups] window, click [Advanced].

Creating Folder Shares

- Specify one or more object types, select a location, and then click [Find Now].
- From the list of results, select the groups and users you want to grant access to, and then click [OK].
- In the [Select Users or Groups] window, click [OK].
- In the [Groups or user names:] list, select a group or user, and then, in the [Allow] column of the permissions list, select either the [Full Control] or [Change] checkbox.
- Configure the access permissions for each group and user.
- Click [OK].
- Select the [Security] tab, and then configure the access permissions.
- Add to the list the groups and users whom you want to grant access to, and then configure the access permissions for each. The procedure is the same as the procedure explained in steps 6 through 11.
- Click [OK].

Creating Folder Shares

Step 2: Confirming the user name and computer name

- Confirm the user name and the name of the computer you will send scanned documents to.
- **On the [Start] menu, point to [All Programs], then [Accessories], and then click on [Command Prompt].**
- The command prompt window opens.
- **Enter the command “ipconfig/all”, and then press the [Enter] key.**
- **Confirm the name of the computer.**
- The computer's name is displayed under [Host Name].
- You can also confirm the IPv4 address. The address displayed under [IP Address] is the IPv4 address of the computer.

Creating Folder Shares

- **Next, enter the command "set user", and then press the [Enter] key. (Be sure to put a space between "set" and "user".)**
- **Confirm the user name.**
- The user name is displayed under [USERNAME].

Depending on the operating system or security settings, it might be possible to specify a user name that does not have a password assigned. However, we recommend that for greater security you select a user name that has a password.

Configuring File and Share Access Permissions

Assigning Permissions

- Normally, you do not have to worry about permissions in Windows because that's already taken care of by the operating system. Each user has their own profile and their own set of permissions, which prevents unauthorised access to files and folders.
- There are times, however, when you might want to manually configure the permissions on a set of files or folders in order to prevent other users from accessing the data. This post is assuming the other "people" also have access to the same computer you are using.

Assigning Permissions

Permission Types

- There are basically six types of permissions in Windows: **Full Control**, **Modify**, **Read and Execute**, **List Folder Contents**, **Read**, and **Write**. **List Folder Contents** is the only permission that is exclusive to folders.

Configuring File and Share Access Permissions

Assigning Permissions

Permission	Meaning for Folders	Meaning for Files
Read	Permits viewing and listing of files and subfolders	Permits viewing or accessing of the file's contents
Write	Permits adding of files and subfolders	Permits writing to a file
Read & Execute	Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders	Permits viewing and accessing of the file's contents as well as executing of the file
List Folder Contents	Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only	N/A
Modify	Permits reading and writing of files and subfolders; allows deletion of the folder	Permits reading and writing of the file; allows deletion of the file
Full Control	Permits reading, writing, changing, and deleting of files and subfolders	Permits reading, writing, changing and deleting of the file

Assigning Permissions

Please follow through.

- In Windows Explorer, **right-click** the file or folder you want to work with.
- From the pop-up menu, select **Properties**, and then in the Properties dialogue box click the **Security tab**.
- In the Name list box, select the **user, contact, computer, or group** whose permissions you want to view. If the permissions are dimmed, it means the permissions are inherited from a parent object.
- **Turn off UAC (User Account Control)**

Before you can do anything, you must turn off the UAC, or you will be locked out of the following steps.

1. Start -> Settings -> Control Panel -> User Accounts.
2. Click "Change User Account Control Settings“.
3. Move slider all the way down to "Never Notify“.
4. Reboot.

Assigning Permissions

2. **Take Ownership**
   Yes, take ownership. Even though you are logged on as an Administrator, you cannot change files that do not belong to you. The Program Files folder is set to the Trusted Installer group, and the Administrator does not have the rights to change anything. So now we have to claim all the files and folders.
   1. Open Windows Explorer
   2. R-Click on Program Files -> Properties -> Security Tab
   3. Click Advanced -> Owner
   4. Click Edit
   5. Select Administrators -> Put a checkmark in Replace owner on sub-containers and objects -> Apply
   6. Wait a while,
   7. When it finishes, Click OK on all boxes to close everything

Assigning Permissions

3. **Fix Permissions**

   Now that you own the files, you have to give yourself permission to modify them

   1. R-Click on Program Files -> Properties -> Security Tab
   2. Click Advanced -> Change Permission
   3. Select Administrators (any entry) -> Edit
   4. Change the Apply To drop-down box to This Folder, Subfolder & Files
   5. Put check in Full Control under Allow column -> OK -> Apply
   6. Wait some more,
   7. When it finishes, the dialogue boxes may hide behind the Explorer window. Minimise it and click OK on all the dialogue boxes
   8. Reboot PC.

Configuring File and Share Access Permissions

Understanding the windows Permission Architecture and Basic

- In any Windows network, you can set sharing permissions for drives and folders. On that network, each user can choose to share entire drives or individual folders with the network.
- NTFS (NT File System) permissions are available to drives formatted with NTFS. The advantage with NTFS permissions is that they affect local users as well as network users and they are based on the permission granted to each individual user at the Windows logon, regardless of where the user is connecting.
- Administrators can use the NTFS utility to provide access control for files and folders, containers and objects on the network as a type of system security. Known as the "Security Descriptor", this information controls what kind of access is allowed for individual users and groups of users.

Understanding the windows Permission Architecture and Basic

Share permissions for files and folders

- The following are levels of share permissions:
- **Read:** This is the default permission for any file that is shared in Windows Server 2003. With Read permissions, a user can see a file or folder and can execute the file or open the folder. A user can also right-click the file or folder and view the properties, but cannot make any changes to the file or folder or to its properties.
- **Change:** Change permissions allow all of the permissions of Read, but the user can also change or add to the file or folder and can change the properties of the file or folder, such as the name or other attributes. In addition, the user can also delete the file or folder with Change permissions.
- **Full Control:** Full Control permissions allow all of the permissions of Change, and the user can take ownership of the file or folder and, thereby, assign other users permission for the file or folder.

Understanding the windows Permission Architecture and Basic

- Modern Unix systems may support other forms of permissions. Most modern Unix systems (Solaris, Linux, *BSD) support access control lists which allow assigning read/write/execute permissions for more than one user and more than one group for each file. The filesystem must have room to store this extra information, and the kernel must include code to look up and use this information. Ext2, ReiserFS, btrfs, zfs, and most other modern Unix filesystem formats define a place to store such ACLs. Mac OS X supports a different set of ACL which include non-traditional permissions such “append” and “create a subdirectory”; the HFS+ filesystem format supports them. If you mount an HFS+ volume on Linux, these ACLs would not be enforced since the Linux kernel doesn't support them.

Configuring File and Share Access Permissions

Understanding the windows Permission Architecture and Basic

- The permissions themselves are different. In NetWare, there were only 7 rights you could choose from: Read, Write, Create, Erase, Modify, File Scan, and Access Control. Aside from Modify and File Scan, these were reasonably self-explanatory.
- In Windows, there are a lot more (between 13 and 19, depending on what you count). They are:
- Full Control

  Traverse Folder/Execute File

  List Folder/Read Data

  Read Attributes

  Read Extended Attributes

  Create Files/Write Data

  Create Folders/Append Data

  Write Attributes

  Write Extended Attributes

  Delete Subfolders and Files

  Delete

  Read Permissions

  Change Permissions

  Change Ownership

  Synchronise

Understanding the windows Permission Architecture and Basic

- Permissions define the type of access that is granted to a user or group for an object or object property. For example, the Finance group can be granted Read and Write permissions for a file named Payroll.dat.
- By using the access control user interface, you can set NTFS permissions for objects such as files, Active Directory objects, registry objects, or system objects such as processes. Permissions can be granted to any user, group, or computer. It is a good practice to assign permissions to groups because it improves system performance when verifying access to an object.
- For any object, you can grant permissions to:
- Groups, users, and other objects with security identifiers in the domain.
- Groups and users in that domain and any trusted domains.
- Local groups and users on the computer where the object resides.

Understanding the windows Permission Architecture and Basic

- The permissions attached to an object depend on the type of object. For example, the permissions that can be attached to a file are different from those that can be attached to a registry key. Some permissions, however, are common to most types of objects. These common permissions are:
  - Read
  - Modify
  - Change owner
  - Delete
- When you set 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.
- When you need to change the permissions on a file, you can run Windows Explorer, right-click the file name, and click **Properties**. On the **Security** tab, you can change permissions on the file.

Advanced Permissions, Allowing and Denying Permissions, Inheriting Permissions

Advanced Permissions

- Advanced permissions are the detailed permissions that are grouped together to create standard permissions. Since advanced permissions are used in combinations to create standard permissions, there are more of them overall. For a file, here is a list of the advanced permissions:
- Full Control
  - Traverse Folder/Execute File.
  - List Folder/Read Data.
  - Read Attributes.
  - Read Extended Attributes.

Advanced Permissions

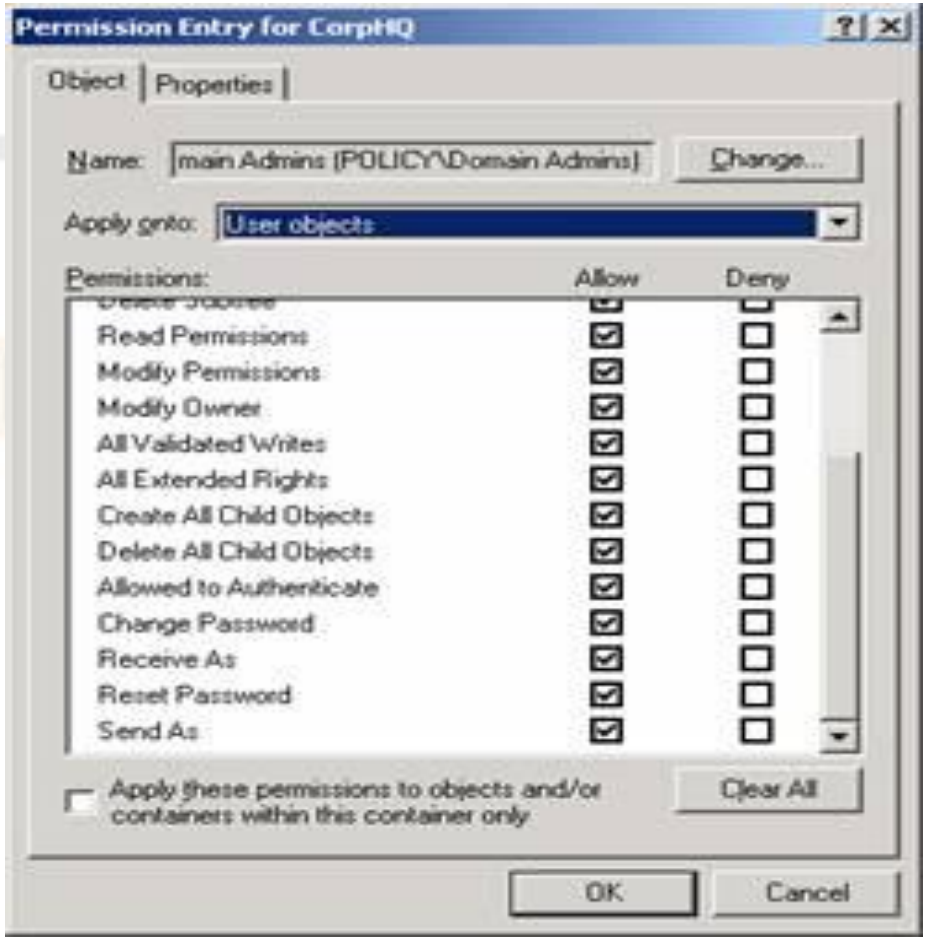
- Create Files/Write Data
- Create Folders/Append Data
- Write Attributes
- Write Extended Attributes
- Delete
- Read Permissions
- Change Permissions
- Take Ownership

For example, the specific advanced permissions that are used to create the Read standard permission include:

- List Folder/Read Data.
- Read Attributes.
- Read Extended Attributes.
- Read Permissions.

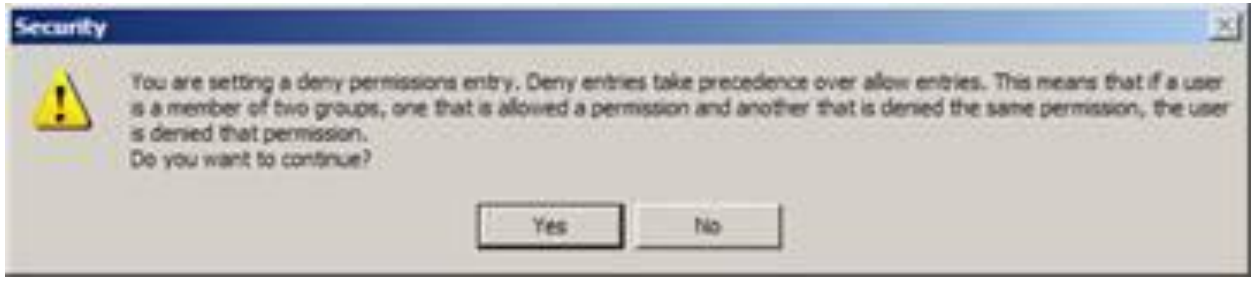
Advanced Permissions

- When you evaluate the advanced permissions for a folder, they are identical to those of a file. However, when you investigate the advanced permissions of a printer or Registry key, they are completely different. If you want to see the power and control that NTFS 5.0 provides for access control, it is best to investigate the permissions of an OU within Active Directory. Upon first glance, I calculate that you have over 10,000 individual advanced permissions that you can set for an OU(Organisational Unit).



Allowing and Denying Permissions

- When establishing permissions, you need to specify whether the entry should have access (Allow) or not (Deny) to the resource. The Local Security Authority (LSASS) then controls the access to the resource, based on the security ID (SID) that you placed on the ACL to the SID placed on the security token that is given to the user at logon. If the SID associated with the user is on the ACL, the LSASS must determine whether the access is set to Allow or Deny. The Allow and Deny permissions inherit down through the structure as described in the section above on inheritance. You will get warnings from the ACL editor when you create Deny entries, as shown in Figure



Allowing and Denying Permissions

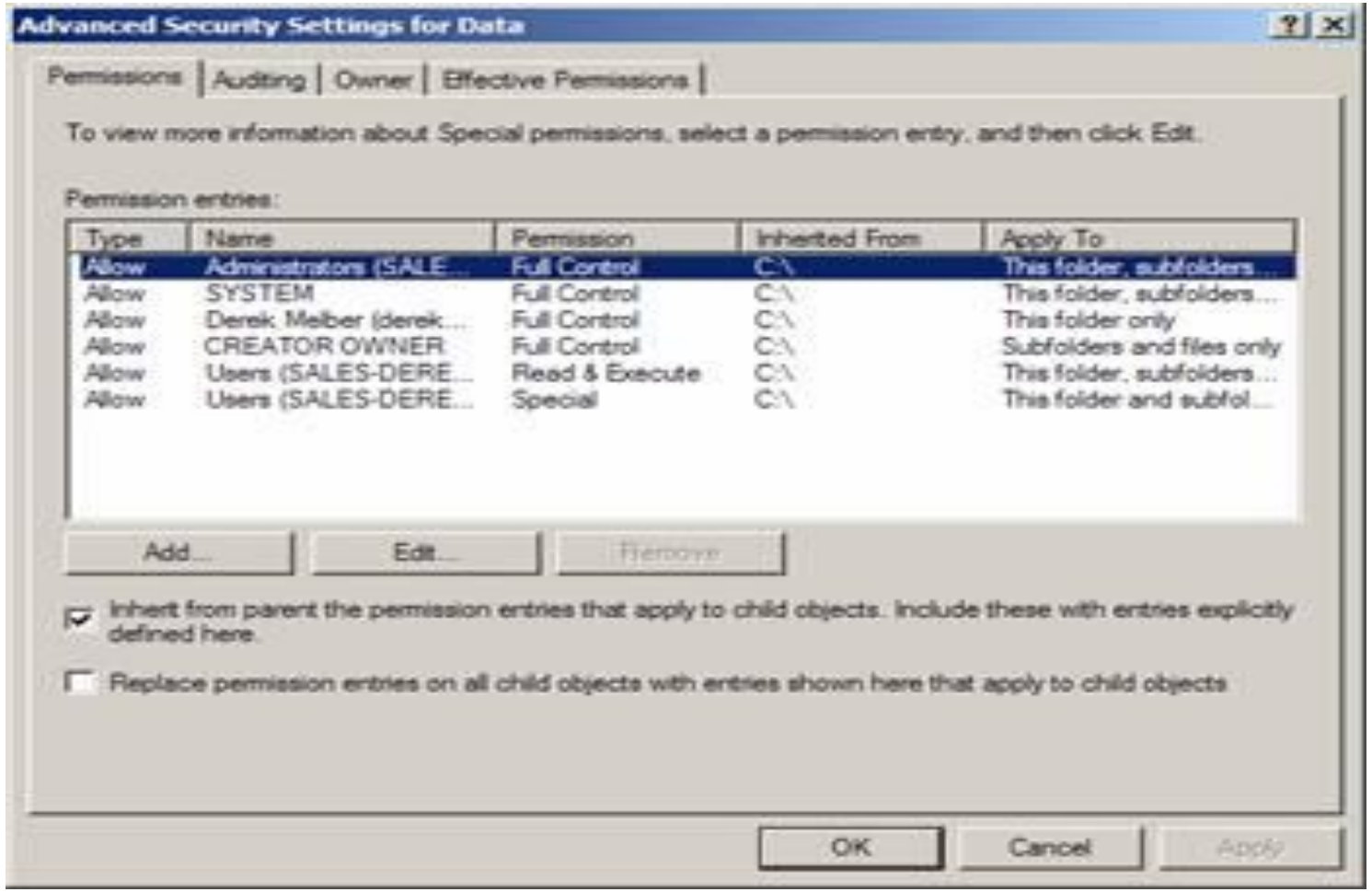
- It is not common to configure resources with Deny permissions, because of the nature of how permissions are evaluated. It is more common to exclude the user or group from the ACL instead of configuring them to have explicit Deny permissions.
- The fact that the user or group SID is not on the ACL will have the same result of "No Access" to the resource, without needing to configure any special entries on the ACL.
- It is only in the rare instance that a user or group should be explicitly denied access that you configure Deny permissions. Denial of access to resources by omission from the ACL is easier to troubleshoot, manage, and configure.

Inheriting Permissions

- There are two variations of permissions that you will see for anyone entry (user, computer, or group) listed on the access control list (ACL). If we look at the root drive, C: you can add or modify the permissions for any entry on the ACL.
- If you create a new folder under C, say a new folder named Data (C:\Data), you won't be able to modify the permissions for any existing entries. This is because the permissions from C: inherit down to all subfolders and files automatically.
- If you don't want the permissions from C: to inherit down the C:\Data, but still want them to inherit down to other subfolders below C:, you would configure the C:\Data folder to stop inheriting by removing the check from the "Inherit from parent the permission entries that apply to child objects.

Configuring File and Share Access Permissions

Inheriting Permissions



Inheriting Permissions

- When you are working with permissions, you can easily determine whether permission is inherited. Inherited permissions are shaded (unavailable) and directly assigned permissions are not shaded. If you do not want a file or a folder to have the same permissions as a parent folder, you have several choices. You can:
- Access the parent folder and configure the permissions you want all included files and folders to have.
- Try to override inherited permission by selecting the opposite permission. In most cases, Deny overrides Allow.
- Stop inheriting permissions from the parent folder and then copy or remove existing permissions as appropriate.

Inheriting Permissions

- If you want a file or a folder to stop inheriting permissions from a parent folder, follow these steps:
- In Windows Explorer, right-click the file or folder you want to work with and then select Properties.
- In the Properties dialogue box, select the Security tab and then click Advanced. This opens the "Advanced Security Settings for" dialogue box.
- On the Permissions tab, click Change Permissions. This opens an editable view of the Permissions tab in a new dialogue box.
- Clear the "Include inheritable permissions from this object's parent" checkbox.
- In the Windows Security dialogue box, click Add to convert and add the permissions that were applied previously through inheritance, or click Remove to remove the inherited permissions and apply only the permissions that you explicitly set on the folder or file.
- After you modify or remove additional permissions as necessary, click OK to save your settings.

Understanding Effective Access, Setting Share Permissions, Understanding NTFS Authorization, Assigning Basic NTFS Permissions

Understanding Effective Access

- NTFS effective permissions are the resultant permissions of a file or folder for a user or group. It is the combination of explicit and inherited permissions on an object. In other words, its the permissions a user or group has to a file or folder.
- When trying to determine the effective permissions you need to consider the following:
  - Group Membership.
  - Inherited Permissions.
  - Nested groups.
  - Explicit deny permissions.
  - Local group membership.

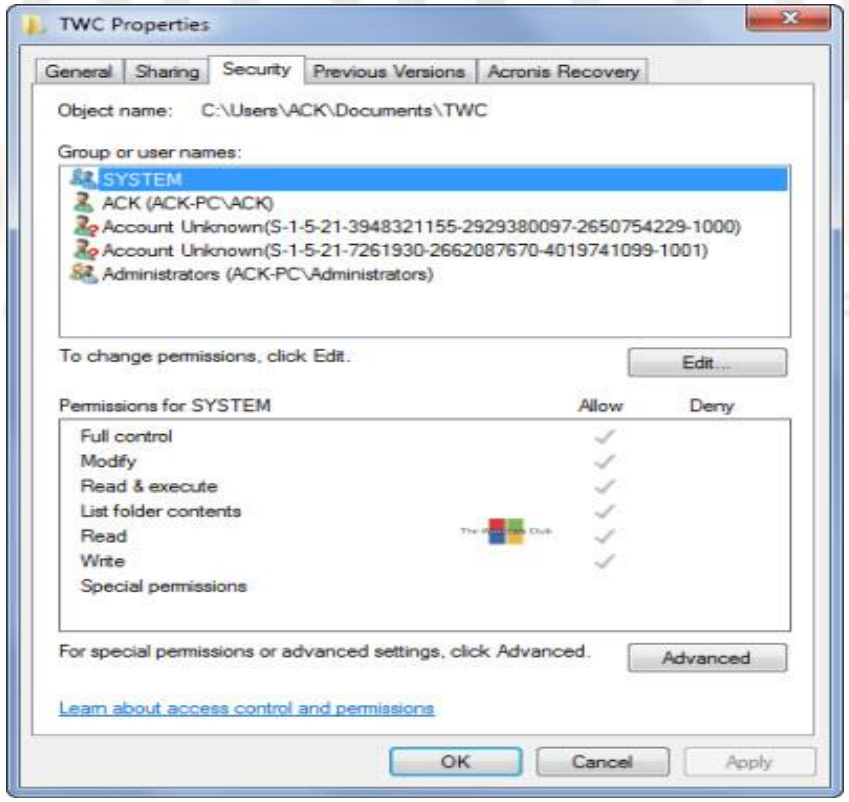
Understanding Effective Access

- When you create a new file or folder, it will either take the operating systems defaults or inherit permissions from a parent folder.
- Seems straightforward right? Yes and No
- Depending on how your network shares are structured and how granular you get with access, it can become a big tangled mess.
- Effective Permissions is a set of permissions of the file or folder for any user or user group. To secure the contents of the user, Windows sets some permission for each file or folder objects. It grants users specific user rights that will allow the user or user group to read, modify, delete, etc. the object. The minimum permission is the Read permission.

Understanding Effective Access

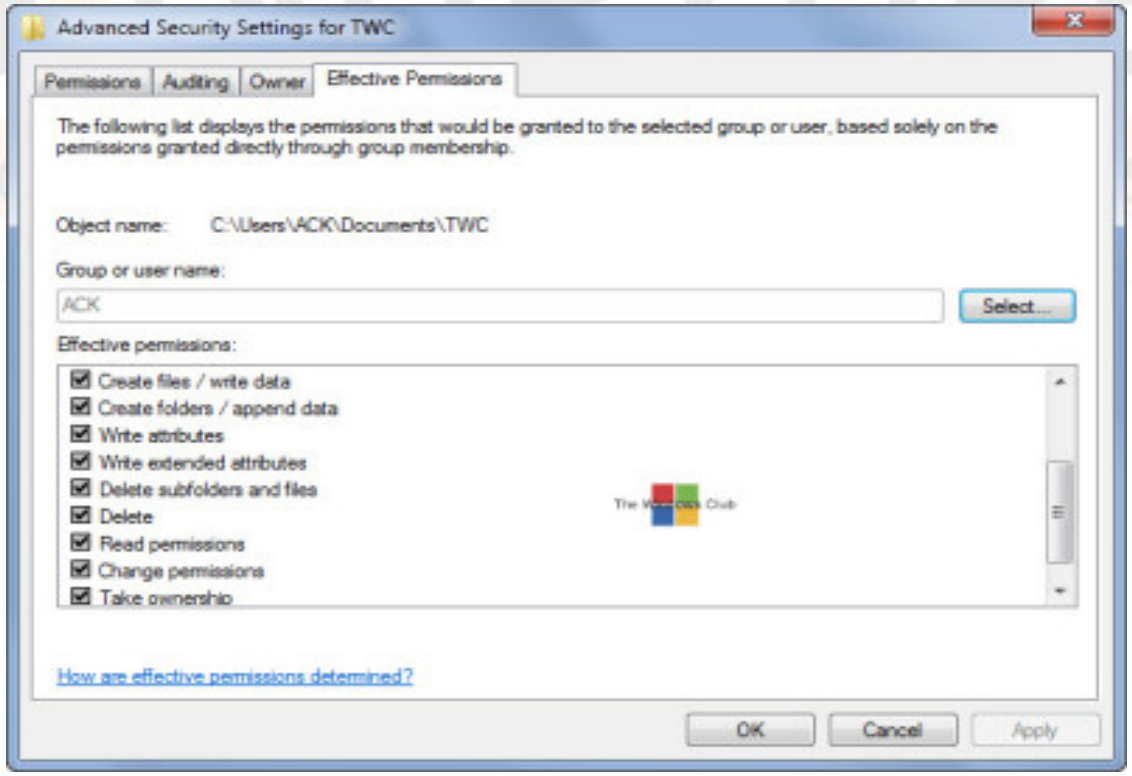
View Effective Permissions for User or User Groups

1. To view the Effective Permissions for any files or folders, right-click on it and select Properties and click on the Security tab.



Understanding Effective Access

2. Next, click on the Advanced button and then on the Effective Permissions tab.
3. Now click on Select.
4. Here, enter the name of a user or user group and click on OK.



Configuring File and Share Access Permissions

Setting Share Permissions

- Share permissions manage access to folders shared over a network; they do not apply to users who log on locally. Share permissions apply to all files and folders in the share; you cannot granularly control access to subfolders or objects on a share. You can specify the number of users who are allowed to access the shared folder. Share permissions can be used with NTFS, FAT and FAT32 file systems.
- There are three types of share permissions: Full Control, Change and Read. You can set each of them to “Deny” or “Allow” to control access to shared folders or drives.

Setting Share Permissions

- **Read** — Users can view file and subfolder names, read data in files, and run programs. By default, the “Everyone” group is assigned “Read” permissions.
- **Change** — Users can do everything allowed by the “Read” permission, as well as add files and subfolders, change data in files, and delete subfolders and files. This permission is not assigned by default.
- **Full Control** — Users can do everything allowed by the “Read” and “Change” permissions, and they can also change permissions for NTFS files and folders only. By default, the “Administrators” group is granted “Full Control” permissions.

Setting Share Permissions

- **Setting Permissions**
- Use Windows Explorer to locate the file or folder for which you want to edit the permissions.
- Right-click the folder, and then click Properties.
- Click the Security tab.
- To add a new access control setting to the folder, click Add.
- Select the users, computers, or groups that this access control setting is applied to, click Add, and then click OK.
- To remove an access control setting, click Remove.
- To edit the permissions for any group, select the user or group, and then use the corresponding check boxes in the Permissions pane.
- Click OK to accept the settings, click Cancel to cancel any changes you have made or click Apply to apply the changes without closing the file or folder properties.

Setting Share Permissions

How to Change Share Permissions

- To change share permissions:
- Right-click the shared folder.
- Click “Properties”.
- Open the “Sharing” tab.
- Click “Advanced Sharing”.
- Click “Permissions”.
- Select a user or group from the list.
- Select either “Allow” or “Deny” for each of the settings.

Understanding NTFS Authorization

- Because of the fact that users have can have many different rights settings, and objects can have many different permission settings, it is possible that conflicting permission settings might apply to a particular object and access method.
- When this occurs, the system must engage in a process of resolving the various permissions to determine which ones should govern the access.

Here are some rules for resolving permissions conflicts:

- "Deny" permissions generally take precedence over "allow" permissions.
- Permissions applied directly to an object (explicit permissions) take precedence over permissions inherited from a parent (**for example,** from a group).

Understanding NTFS Authorization

- Permissions inherited from near relatives take precedence over permissions inherited from distant predecessors. So permissions inherited from the object's parent folder take precedence over permissions inherited from the object's "grandparent" folder, and so on.
- Permissions from different user groups that are at the same level (in terms of being directly-set or inherited, and in terms of being "deny" or "allow") are cumulative. So if a user is a member of two groups, one of which has an "allow" permission of "Read" and the other has an "allow" or "Write", the user will have both read and write permission--depending on the other rules above, of course.

Understanding NTFS Authorization

- Although Deny permissions generally take precedence over allow permissions, this is not always the case. An explicit "allow" permission can take precedence over an inherited "deny" permission.
- The hierarchy of precedence for the permissions can be summarised as follows, with the higher precedence permissions listed at the top of the list:
- Explicit Deny.
- Explicit Allow.
- Inherited Deny.
- Inherited Allow.

Understanding NTFS Authorization

- There are seven listings for permissions. They are Full Control, Modify, Read & Execute, List Folder Contents, Read, Write, and Special Permissions. With the exception of the latter, these permissions allow users varying degrees of access. The allowed access at each level is as follows:
- Read - This allows users the ability to list folders, read files, read attributes, and read permissions. It will not allow users to execute executables and scripts.
- Write - This allows users to create files, write data, create folders, and set attributes.
- List Folder Contents - This allows users to view folder contents but does not allow them to read files.
- Read & Execute - This allows users to traverse directories and read all files and folders as well as execute executables and scripts.
- Modify - This allows users to Write, Read, Execute, and Traverse.
- Full Control - This allows users to have full control over all files, folders, permissions, attributes, and ownership.
- Special Permissions - This is a greyed-out checkbox that indicates whether or not there are any special permissions given to the specified user

Assigning Basic NTFS Permissions

- Permissions are grouped in order to make it easier to assign complimentary permissions to users. These groups are called "basic" permissions. The table below shows how permissions are assigned to basic permissions in each case.

Assigning Basic NTFS Permissions

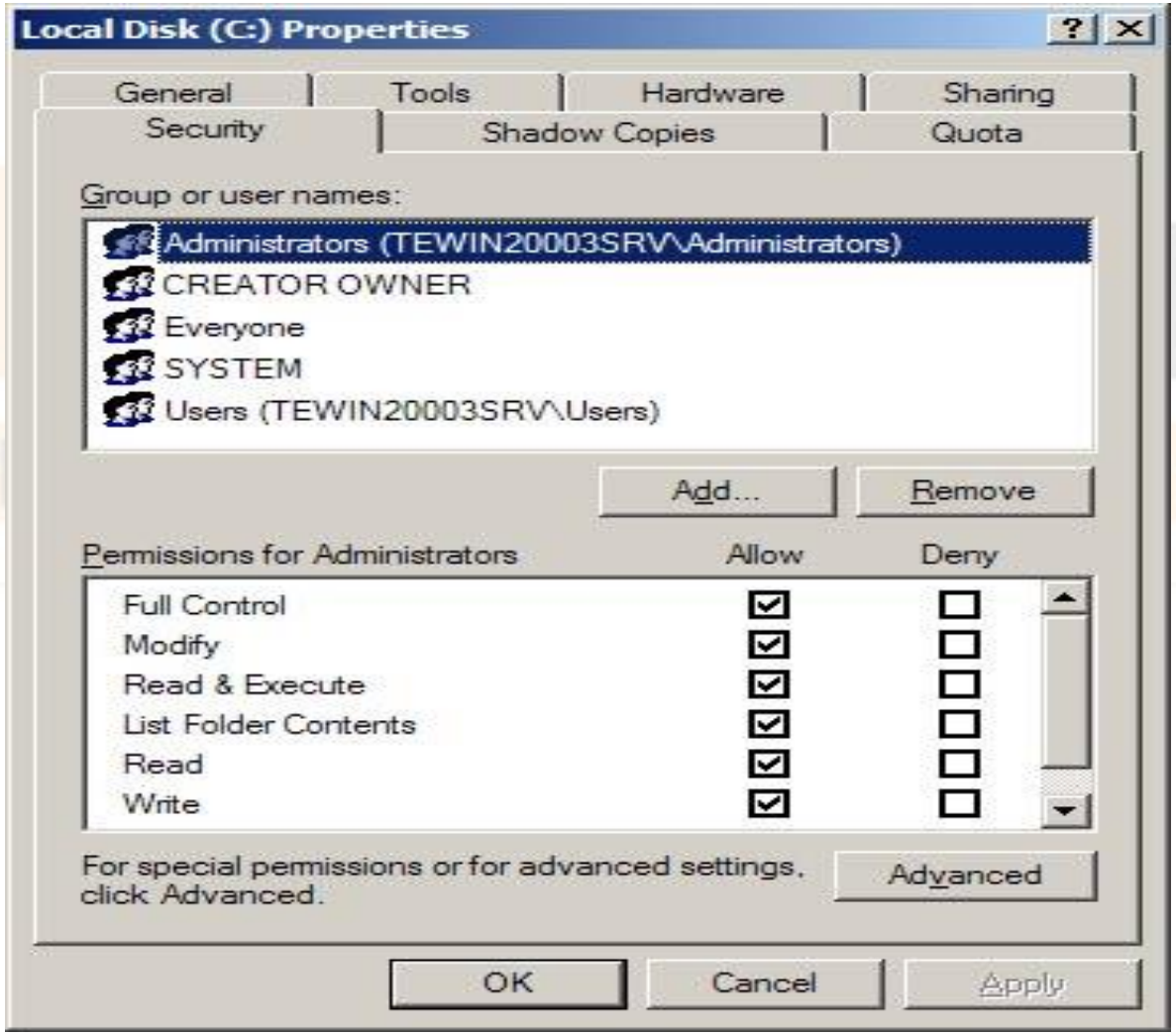
Permissions	Basic Full Control	Basic Modify	Basic Read & Execute	Basic List Folder Contents	Basic Read	Basic Write
Travers Folder/Execute File	✖	✖	✖	✖		
List Folder/ Read Data	✖	✖	✖	✖	✖	
Read Attributes	✖	✖	✖	✖	✖	
Read Extended Attributes	✖	✖	✖	✖	✖	
Create Files/Write Data	✖	✖				✖
Create Folders/Append Data	✖	✖				✖
Write Attributes	✖	✖				✖
Write Extended Attributes	✖	✖				✖
Delete Subfolders and Files	✖					
Delete	✖	✖				
Read Permissions	✖	✖	✖	✖	✖	✖
Change Permissions	✖					
Take Ownership	✖					
Synchronize	✖	✖	✖	✖	✖	✖

Assigning Basic NTFS Permissions

- **Setting NTFS Permissions**
- The most common way to set permissions is to use Windows Explorer.
- To set permissions for an object:
  - In Windows Explorer, right-click a file, folder or volume and choose **Properties** from the context menu. The **Properties** dialogue box appears.
  - Click the **Security** tab.
  - Under **Group or user names**, select or add a group or user.
  - At the bottom, allow or deny one of the available permissions.
  - **Properties dialogue box showing Security tab.**

Configuring File and Share Access Permissions

Assigning Basic NTFS Permissions



Understanding Resource Ownership, Combining Share and NTFS Permissions, Installing File Server Resource Manager

Understanding Resource Ownership

- In Windows, ownership is power—a user who creates an object automatically becomes its owner and can set permissions at his or her discretion. This authorisation model, known as discretionary access control (DAC), means an object owner can control access to a file, folder, registry key or Active Directory (AD) object, affecting the availability of that data as well as your organization's efforts to comply with regulatory requirements.

- Windows implicitly grants an object owner read permissions and change permissions on the object, which means that the owner is always allowed to access the object, regardless of what the object's ACL says. These implicit permissions do not show up in the object's ACL. Even if the object's ACL includes an explicit deny Access Control Entry (ACE) for the owner’s user account, the owner can still access the object’s ACL and override or simply remove the deny ACE. If you do detect explicit ACEs for the object owner in the object's ACL, these are not related to the implicit owner permissions but to ownership inheritance.

Understanding Resource Ownership

- Assigning ownership to a group rather than to the individual who created the object is not good from an accountability and traceability point of view. An admin could leverage it to hide his or her object creation tracks. That's why Windows XP and Windows Server 2003 include a configurable option to control such behaviour.
- In Windows 2003, XP, and Win2K, the Administrators group is also the default owner of Windows files and folders. These include all files and folders that are created as part of the Windows installation process

How to take ownership

- Open-**File Explorer**.
- Browse and find the file or folder you want to have full access.

Understanding Resource Ownership

- Right-click it, and select **Properties**.
- Click the **Security** tab to access the NTFS permissions.
- Click the **Advanced** button.
- On the "Advanced Security Settings" page, you need to click the **Change** link, in the Owners field.
- Click the **Advanced** button.
- On the "Select User or Group" page, click the **Find Now** button.
- From the search result, select your user account, and click **OK**.
- On the "Select User or Group" page, click **OK**.

Understanding Resource Ownership

- Click **Apply**.
- Click **OK**.
- Click **OK** again.
- Click **OK** one more time to complete this task.
- It's important to note that if you are taking ownership of a folder, you can check the **Replace ownership on sub-containers and object** option in the Advanced Security Settings page to take control of the subfolders inside of the folder.
- Now you will need to grant full access control to your account, to do this use the following steps:

Understanding Resource Ownership

- Right-click the file or folder and select **Properties**.
- Click the **Security** tab to access the NTFS permissions.
- Click the **Advanced** button.
- Under the Permissions tab, click **Add**.
- Click **Select a principal** to add your user account.
- On the "Select User or Group" page, click the **Find Now** button.
- From the search result, select your user account, and click **OK**.
- On the "Select User or Group" page, click **OK**.
- On "Permission Entry", check the **Full control** option.
- Click **OK**.

Understanding Resource Ownership

- Click **OK**.
- Click **Apply**.
- Click **OK**.
- Click **OK** to close the file or folder properties to complete the task.
- It is important to note that if you're taking ownership of a folder, you can check the **Replace all existing inheritable permissions on all descendants with inheritable permissions for this object** option in the Advanced Security Settings page to replace the subfolders permissions with the settings from the parent folder.

Combining Share and NTFS Permissions

Rules for combining permissions

- When working within a certain permission type (sharing or NTFS), permissions are cumulative. The most lenient setting wins for a particular user or group. Deny always overrides Allow and negates any permission with which it conflicts
- When there's a difference between the sharing permission and the NTFS permission, the most restrictive setting wins
- Permissions are not cumulative across groups; each group's permission is calculated separately. For example, if a user is a member of Group A, which has Full Control sharing permission but no NTFS permission for an object, and also of Group B, which has Full Control NTFS permission but no sharing permission for the object, that user has no permission for the object.

Combining Share and NTFS Permissions

- One strategy for providing access to resources on an NTFS volume is to share folders with the default shared folder permissions and then control access to shared folders by assigning NTFS permissions. When you share a folder on an NTFS volume, both shared folder permissions and NTFS permissions combine to secure file resources.
- Shared folder permissions provide limited security for resources. You gain the greatest flexibility by using NTFS permissions to control access to shared folders. Also, NTFS permissions apply whether the resource is accessed locally or over the network.

Combining Share and NTFS Permissions

Planning

- The first step is planning how folders will be shared. To do this, make a list of what data will be stored and what user groups will require access. For example, types of data may be employee data, customer account status data, customer service data, management guideline data, and so on. Groups of users may be managers, administrators, sales reps, customer service reps, and so on.
- Create a table with three columns:
- Column 1 displays each data folder by name and location
- Column 2 displays the shared folder name
- Column 3 displays the name of the user group with assigned folder permissions
- File and Printer Sharing for Microsoft Networks

Combining Share and NTFS Permissions

- To share any folders or other network objects, you must have "File and Printer Sharing for Microsoft Networks" as a networking component in your local area connection.

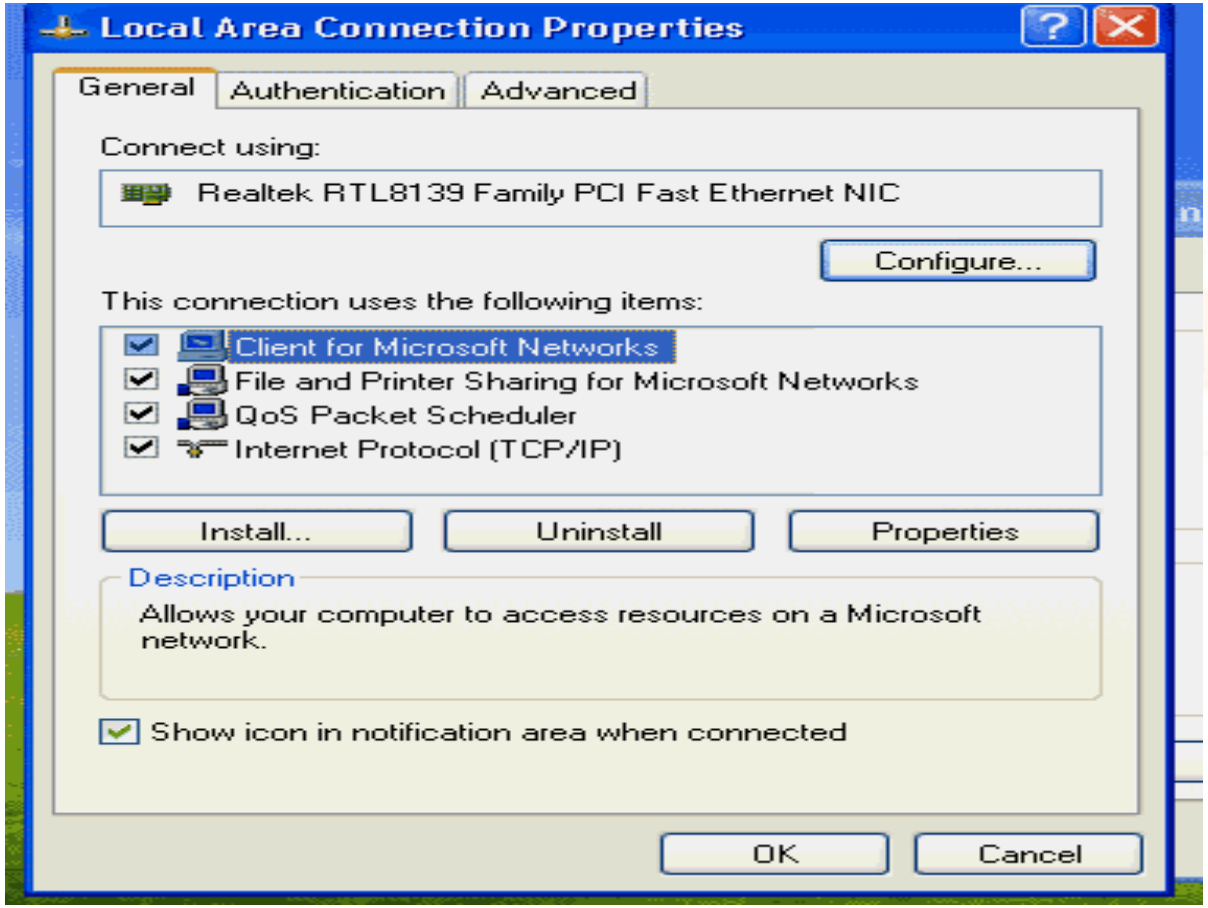
To add this component:

- In the Windows System Tray, right-click the Local Area Connection icon and choose Status from the context menu. The Local Area Connection Status dialogue box appears.
- Click Properties. The Local Area Connection Properties dialogue box appears.

  Local Area Connection Properties dialogue box
- To add the **File and Printer Sharing for Microsoft Networks** check box, click **Install…** and choose it from the **Services** category.

Combining Share and NTFS Permissions

- Select the **File and Printer Sharing for Microsoft Networks** check box and click **OK**.



Installing File Server Resource Manager

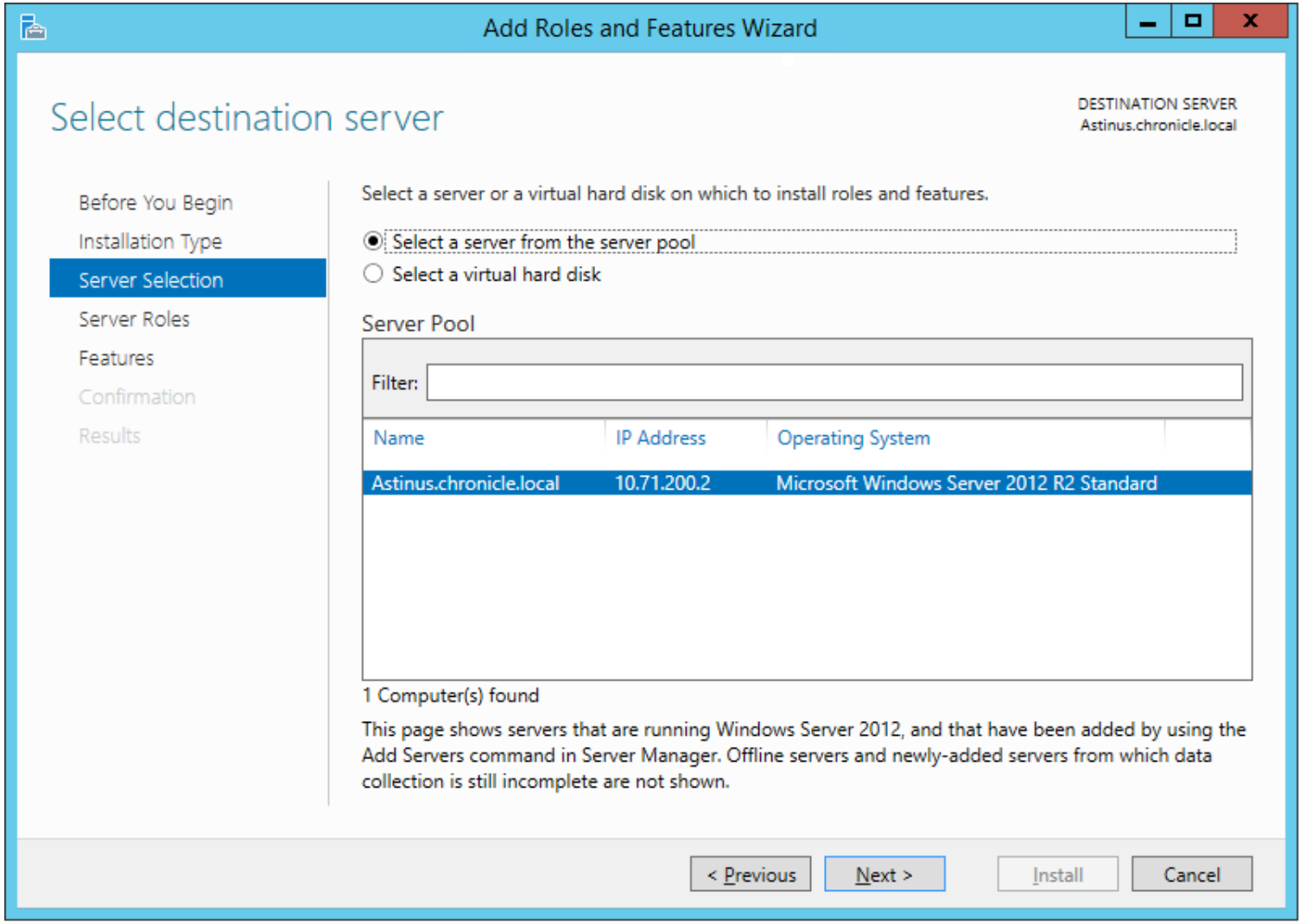
- Microsoft File Server Resource Manager is a suite of tools from Microsoft that allows administrators to better understand, control, and manage the quantity and type of data stored on their servers. Storage Manager uses File Server Resource Manager to enable quota management.
- You must install FSRM on all servers where Storage Manager will be managing quotas, including the server that will host the Engine. Even if the Engine host does not contain shares that will be managed, FSRM is still required because the FSRM COM interfaces must be present for the Engine to call them remotely on other servers.
- These procedures are specific to Windows Server 2012 R2. Procedures vary for each version of Windows Server.

Installing File Server Resource Manager

- Launch Server Manager.
- Select **Manage** > **Add Roles and Features**.
- This launches the Add Roles and Features Wizard.
- Click **Next**.
- Select the server where you are going to install the Engine and click **Next**.
- From the list of roles, expand **File and Storage Services.**
- Expand **File and iSCSI Services**.
- Select the **File Server Resource Manager** check box.
- Click **Add Features**. Click **Next**. Click **Next**. Click **Install**.

Configuring File and Share Access Permissions

Installing File Server Resource Manager



Using, creating, changing Quotas, Managing Files with File Screening, Creating File Groups, Creating a File Screen, Creating a File Screen Exception

Configuring File and Share Access Permissions

Using, creating, changing Quotas, Managing Files with File Screening

- File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers.
- By using File Server Resource Manager, administrators can place quotas on volumes, actively screen files and folders, generate comprehensive storage reports, control the File Classification Infrastructure, and use file management tasks to perform scheduled actions on sets of files.
- This set of advanced instruments helps the administrator efficiently monitor existing storage resources, and it aids in planning and implementing future policy changes.

Configuring File and Share Access Permissions

Using, creating, changing Quotas, Managing Files with File Screening

- File Screening Management allows you to create file screens to block types of file from being saved on a volume or in a folder tree.
- A file screen affects all folders in the designated path. You use file groups to control the types of files that file screens manage. For example, you might create a file screen to prevent users from storing audio and video files in their personal folders on the server. Like all components of FSRM, you can choose to generate an email or other notifications when a file screening event occurs.
- For this demo, as usual, I will be using my **DC01.comsys.local, SVR01.comsys.local and my Surface01.comsys.local client PC.**

Configuring File and Share Access Permissions

Using, creating, changing Quotas, Managing Files with File Screening

- Before you started using FSRM and manage it, you need to **install the FSRM**.
- On the SVR01.comsys.local (this is my File Server), open Server Manager, on the Dashboard click Add Roles and Features, and click 2 times until you reach Select server roles box.
- On the Select server roles box, expand File and Storage Services (Installed), expand File and SCSI Services, and then select the **File Server Resource Manager checkbox then click Add Features.**
- Next, On the Select server roles box click **Next** to proceed.
- On the Select Features box, click **Next** to proceed.
- On the Confirm installation selections box, click Install and **wait a few minutes for the installation to be completed.**

Using, creating, changing Quotas, Managing Files with File Screening

- When the installation completes, click **Close**.
- Next, **open File Server Resource Manager.**
- In the File Server Resource Manager console, expand **File Screening Management, and then click File Group, Right Click File Group and click Create File Group.**
- In the Create File Group Properties window, in the File group name box, **type Comsys Media Files, then in the Files to include box, type *.mp* and *.torrent, and then click Add, in the Files to exclude box, type *.docx and *.xlsx, click Add, and then click OK.**
- **Verify** that Comsys Media Files available in the File Group list.
- Next, let us **create a File Screen Template**, right-click File Screen Template, and click Create a File Screen Template.

Using, creating, changing Quotas, Managing Files with File Screening

- In the Create File Screen Template box, **under Template name: type Comsys Media, then under File Group, select Comsys Media Files check box and next click Event Log tab.**
- Once you click Event Log tab, **click Send a warning to the event log** (this require us to check the event viewer in later exercise) and click OK to continue.
- **Verify** that Comsys Media is listed in the File Screen Template.
- Next step is to **create File Screen**, right-click File Screens, and then click Create File Screen.
- In the Create File Screen box, **in the File screen path text box, type C:\HR**(you can point to any folder that you wish to screen the files), then under Derive properties from this file screen template (recommended) drop-down list box, and then click Comsys Media and then click Create.

Configuring File and Share Access Permissions

Using, creating, changing Quotas, Managing Files with File Screening

- Next, **verify** that the File Screen is pointing to your selected folder…
- Next, let's **test the file screen function,** log in to your client PC, and try copy any MP3 file to HR folder that located in the SVR01 server, you should get a pop up saying that access denied.
- If you have any *.docx or *.xlsx file, please give it a try, since in this demo I exclude *.docx file extension, when my domain users copy any *.docx file, it can be copied into the HR folder.
- Lastly, log in to SVR01 server and open Event Viewer, browse to Windows Logs and click Application, notice that you had the **Warning stated User Comsys\Thava attempted to save C:\HR*.mp3 to C:\HR on the SVR01 server.**
- **Verify also the Event ID is 8215.**

Using, creating, changing Quotas, Managing Files with File Screening

- **Creating a quota**
- The following procedure guides you through the process of creating a quota that is based on a template (this is the recommended practice).
- To create a quota that is based on a template
    1. In Quota Management, click the Quota Templates node.
    2. In the results pane, select the template on which you will base your quota.
    3. Right-click the template and click Create Quota from Template (or click Create Quota from Template in the Actions pane). This opens the Create Quota dialogue box with the summary properties of the quota template displayed.

Using, creating, changing Quotas, Managing Files with File Screening

4. Under Quota path, type or browse to the volume or folder that the quota will apply to.
5. Click the Create quota on path option. Note that the quota properties will apply to the entire volume or folder.
6. Under Derive properties from this quota template, the template you used in step 2 to create your new quota is preselected (or you can select another template from the list). Note that the properties of the template are displayed under Summary of quota properties.
7. Click Create.

changing quotas by editing a quota template

- In Quota Templates, select the quota template that you want to modify.

Using, creating, changing Quotas, Managing Files with File Screening

- Right-click the quota template, and then click Edit Template Properties (or in the Actions pane, under Selected Quota Templates, click Edit Template Properties). This opens the Quota Template Properties dialogue box.
- Perform all necessary changes. The settings and notification options are identical to those that you can set when you create a quota template
- When you are finished editing the template properties, click OK. This opens the Update Quotas Derived from Template dialogue box.
- Select the type of update that you want to apply:

Using, creating, changing Quotas, Managing Files with File Screening

- If you have quotas that have been modified since they were created using the original template, and you do not want to change them, select Apply template only to derived quotas that match the original template. This option updates only those quotas that have not been edited since they were created with the original template.
- If you want to modify all the existing quotas that were created from the original template, select Apply template to all derived quotas.
- If you want to keep the existing quotas unchanged, select Do not apply the template to derived quotas.
- Click OK.

Creating File Groups

- File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various functions such as adding them to Exclusions for AV scans, HIPS monitoring, auto-sandbox rules and so on in Windows Profiles. CDM ships with a set of predefined File Groups and if required administrators can add new File Groups, edit and manage them.
- The 'File Group Variables' tab in the 'Global Variables' interface allows the administrator to view, create and manage pre-defined and custom file groups. The groups added to this interface will be available for selection while configuring Windows Profiles from the 'Profiles' interface.

Creating File Groups

To open the 'File Groups' interface

- Choose 'Settings' from the left and select 'Global Variables‘.
- Click 'File Groups Variables' from the top.
- The list of default and user-defined File groups will be displayed. The default groups are indicated by 'Default' at their right and cannot be edited or deleted.

Sorting, Search and Filter Options

- Clicking on the 'File Groups' column header will sort the items in ascending/descending order of the names of the groups.
- To filter or search for a specific File group, click the search icon at the top right and enter the name of the group on part or full.

Creating File Groups

To add a new File group

- Enter the name shortly describing the group in the 'New File Group' field and click 'Add'.
- The new group will be added to the list. The next step is to add files to the group.
- Click the '+' at the left of the group name.
- Enter the full standard folder/file path of the file to be added to the group in the 'New Path' field and click 'Add‘.
- The file(s) will be added to the group.
- Repeat the process to add more files to the group.

Creating File Groups

- Once a File Group is added, it will be available for selection in applicable settings interfaces for defining the File Groups, example, for adding to 'Exclusions' list in 'Antivirus Settings' panel, in the 'Windows Profile' interface.
- To edit the files in the group, click the 'Edit' icon beside the file name.
- To remove ‘ta’ file added by mistake or an unwanted file from the group, click the trash can icon beside the file name.
- A confirmation dialogue will appear.
- Click 'OK' in the confirmation dialogue.
- **To edit the name of a File Group.**
- Click the 'Edit' icon beside the File Group.

Creating File Groups

- Enter the new name for the group in the 'Rename File Group' dialogue and click 'OK'

To remove a File Group

- Click the Thrash can icon beside the File Group.
- A confirmation dialogue will appear.
- Click 'OK' in the confirmation dialogue.

Note- to do these steps use Comodo Device Manager

Creating File Groups

- When creating a new file screen, you can choose to save a file screen template that is based on the custom file screen properties that you define.
- In **File Screening Management**, click the **File Screens** node.
- Right-click **File Screens,** and click **Create File Screen** (or select **Create File Screen** from the **Actions** pane). This opens the **Create File Screen** dialogue box.
- Under **File screen path**, type the name of or browse to the folder that the file screen will apply to. The file screen will apply to the selected folder and all of its subfolders.
- **How do you want to configure file screen properties**, click **Define custom file screen properties**, and then click **Custom Properties**. This opens the **File Screen Properties** dialogue box.

Creating File Groups

- If you want to copy the properties of an existing template to use as a base for your file screen, select a template from the **Copy properties from template** drop-down list. Then click **Copy**.
- In the **File Screen Properties** dialogue box, modify or set the following values on the **Settings** tab:

  Under **Screening type**, click the **Active screening** or **Passive screening** option. (Active screening prevents users from saving files that are members of blocked file groups and generates notifications when users try to save unauthorised files. Passive screening sends configured notifications, but it does not prevent users from saving files).

Creating File Groups

- Under **Filegroups**, select each file group that you want to include in your file screen (To select the check box for the file group, double-click the file group label).
- If you want to view the file types that a file group includes and excludes, click the file group label, and then click **Edit**. To create a new file group, click **Create**.
- Additionally, you can configure **File Server Resource Manager** to generate one or more notifications by setting options on the **E-mail Message**, **Event Log**, **Command**, and **Report** tabs. For more information about file screen notification options, see Create a File Screen Template.
- After you have selected all the file screen properties that you want to use, click **OK** to close the **File Screen Properties** dialogue box.
- In the **Create File Screen** dialogue box, click **Create** to save the file screen. This opens the **Save Custom Properties as a Template** dialogue box.

Creating File Groups

Select the type of custom file screen you want to create:

- To save a template that is based on these customized properties (recommended), click **Save the custom properties as a template** and enter a name for the template. This option will apply the template to the new file screen, and you can use the template to create additional file screens in the future. This will enable you to later update the file screens automatically by updating the template.
- If you do not want to save a template when you save the file screen, click **Save the custom file screen without creating a template**.

- Click **OK**.

Creating a File Screen Exception

- A file screen exception is a special type of file screen that over-rides any file screening that would otherwise apply to a folder and all its subfolders in a designated exception path. That is, it creates an exception to any rules derived from a parent folder.
- **To create a File Screen Exception**
- In **File Screening Management**, click the **File Screens** node.
- Right-click **File Screens**, and click **Create File Screen Exception** (or select **Create File Screen Exception** from the **Actions** pane). This opens the **Create File Screen Exception** dialogue box.

Creating a File Screen Exception

- In the **Exception path** text box, type or select the path that the exception will apply to. The exception will apply to the selected folder and all of its subfolders.
- To specify which files to exclude from file screening:
  - Under **File groups**, select each file group that you want to exclude from file screening. (To select the check box for the file group, double-click the file group label.)
  - If you want to view the file types that a file group includes and excludes, click the file group label, and click **Edit**.
  - To create a new file group, click **Create**.
- Click **OK**.

Creating a File screen Template and Storage Reports Management

Creating a File screen Template

- A file screen template defines a set of file groups to screen, the type of screening to perform (active or passive), and optionally, a set of notifications that will be generated automatically when a user saves or attempts to save, an unauthorised file.
- By creating file screens exclusively from templates, you can centrally manage your file screens by updating the templates instead of replicating changes in each file screen. This feature simplifies the implementation of storage policy changes by providing one central point where you can make all updates.

Creating a File screen Template

To create a File Screen Template

- In **File Screening Management**, click the **File Screen Templates** node.
- Right-click **File Screen Templates**, and then click **Create File Screen Template** (or select **Create File Screen Template** from the **Actions** pane). This opens the **Create File Screen Template** dialogue box.
- If you want to copy the properties of an existing template to use as a base for your new template, select a template from the **Copy properties from template** drop-down list and then click **Copy**.
- Whether you have chosen to use the properties of an existing template or you are creating a new template, modify or set the following values on the **Settings** tab:
- In the **Template name** text box, enter a name for the new template.

Creating a File screen Template

- Under **Screening type**, click the **Active screening** or **Passive screening** option. (Active screening prevents users from saving files that are members of blocked file groups and generates notifications when users try to save unauthorised files. Passive screening sends configured notifications, but it does not prevent users from saving files).
- To specify which file groups to screen:
- Under **File groups**, select each file group that you want to include (To select the check box for the file group, double-click the file group label).
- If you want to view the file types that a file group includes and excludes, click the file group label, and then click **Edit**. To create a new file group, click **Create**.
- Additionally, you can configure File Server Resource Manager to generate one or more notifications by setting the following options on the **E-mail Message**, **Event Log**, **Command**, and **Report** tabs.

Creating a File screen Template

To configure e-mail notifications:

- On the **E-mail Message** tab, set the following options:
- To notify administrators when a user or application attempts to save an unauthorised file, select the **Send e-mail to the following administrators'** check box, and then enter the names of the administrative accounts that will receive the notifications. Use the format account@domain, and use semicolons to separate multiple accounts.
- To send an e-mail to the user who attempted to save the file, select the **Send e-mail to the user who attempted to save an unauthorised file** check box.
- To configure the message, edit the default subject line and message body that is provided. The text that is in brackets inserts variable information about the file screen event that caused the notification. **For example,** the [**Source Io Owner**] variable inserts the name of the user who attempted to save an unauthorised file. To insert additional variables in the text, click **Insert Variable**.
- To configure additional headers (including From, Cc, Bcc, and Reply-to), click **Additional E-mail Headers**.

Creating a File screen Template

- To log an error to the event log when a user tries to save an unauthorised file:
- On the **Event Log** tab, select the **Send warning to event log** check box, and edit the default log entry.
- To run a command or script when a user tries to save an unauthorised file:
- On the **Command** tab, select the **Run this command or script** check box. Then type the command, or click **Browse** to search for the location where the script is stored. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.
- To generate one or more storage reports when a user tries to save an unauthorised file:
- On the **Report** tab, select the **Generate reports** check box, and then select which reports to generate. (You can choose one or more administrative e-mail recipients for the report or e-mail the report to the user who attempted to save the file.)
- The report is saved in the default location for incident reports, which you can modify in the **File Server Resource Manager Options** dialogue box.
- After you have selected all the file template properties that you want to use, click **OK** to save the template.

Storage Reports Management

- On the **Storage Reports Management** node of the File Server Resource Manager Microsoft® Management Console (MMC) snap-in, you can perform the following tasks:
- Schedule periodic storage reports that allow you to identify trends in disk usage.
- Monitor attempts to save unauthorised files for all users or a selected group of users.
- Generate storage reports instantly.

For example, you can:

- Schedule a report that will run every Sunday at midnight, generating a list that includes the most recently accessed files from the previous two days. With this information, you can monitor weekend storage activity and plan server down-time that will have less impact on users who are connecting from home over the weekend.

Storage Reports Management

- Run a report at any time to identify all duplicate files in a volume on a server so that disk space can be quickly reclaimed without losing any data.
- Run a Files by File Group report to identify how storage resources are segmented across different file groups
- Run a Files by Owner report to analyse how individual users are using shared storage resources.
- Storage Reports is a node on the file server management console that enables system administrators to schedule periodic storage reports that allow the identification of trends in disk usage, look out for any attempts made to save unauthorised files, and generate random reports on demand.

Storage Reports Management

The following are the four ways in which you can use Storage Reports:

- Scheduling a report on a particular day and specific time to generate a list of recently accessed files. Information from these files can help in monitoring weekly storage activities and help in planning on a suitable day to put the server on a downtime for maintenance.
- The report can be used at any given time to identify duplicate files in storage volumes of a particular server. Removing duplicate copies frees up more space.
- A customised file by group report can be used to identify how volumes are distributed across different file groups.
- Run individual file reports to understand how users use shared resources on the network.

Self Assessment Question

1. You are the network administrator for BigCorp (http://www.bigcorp.com) and need to create several new file shares on your server (bigserver.bigcorp.com). Which of the following options can be used for this purpose in a default installation of Windows Server 2003? (Choose three).

    a. Utilise the Computer Management MMC snap-in
    b. Create the file shares within the Windows Explorer
    c. Utilise the Server Management MMC snap-in
    d. Utilise the net share command-line utility
    e. a, b and d

Answer: a, b and d

Self Assessment Question

2. What permissions are granted to the Everyone group over the share created by the following code?

a. change

b. Full control

c. None

d. Read

Answer: Read

Self Assessment Question

3. When calculating final permissions over a file accessed through a remote share, what is the resulting combination composed of Windows PowerShell? (Choose two).

   a. The most restrictive combination of NTFS permissions
   b. The least restrictive combination of NTFS permissions
   c. The most restrictive combination of Share permissions
   d. The most restrictive combination of Share and NTFS permissions
   e. Both b and d

Answer: Both b and d

Self Assessment Question

4. A user has created a network share and assigned the share and NTFS permissions to Full Control and Read & execute. What level of access will users have when accessing the network share?

   a. Full control

   b. Read

   c. No Access

   d. Read and Execute

Answer: Read and Execute

Self Assessment Question

5. Which of the following commands will create a new file with the name ourgroup?

a. file ourgroup

b. touch ourgroup

c. ls ourgroup

d. mkfile ourgroup

Answer: touch ourgroup

Self Assessment Question

6. How many primary and extended partitions are allowed on a hard disk?

a. 1

b. 2

c. 3

d. 4

Answer: 4

Self Assessment Question

7. Which of the following represents read, write, and execute permissions for owner and read and execute for all others?

a. 755

b. 022

c. 733

d. 557

Answer: 755

Self Assessment Question

8. Which command is used to change permissions of a file?

a. chown

b. chperm

c. chgrp

d. Chmod

Answer: Chmod

Self Assessment Question

9. Which command is used to view quota information for a specific user?

a. edquota

b. quota

c. Requota

d. Quotaon

Answer: quota

Self Assessment Question

10. Process of organising data into processed file is classified asNet.exe

a. Deleting a file

b. Organising a File

c. Creating a file

d. Updating a file

Answer: Creating a file

Self Assessment Question

11. A company's administrator has installed the FSRM role service to manage stored data on a file server. The administrator would like to configure quotas limits for users when they create new folders. Which of the following should the administrator configure to enforce quota limits for users when they create new folders?

    a. File group

    b. File quota

    c. File quota template

    d. File screen

Answer: File quota template

Self Assessment Question

12. You are the network administrator responsible for review of shared resources on several servers within a corporate domain. To accomplish this task, you've decided to use an automated script that will run several times per day to determine what shared resources are being used. Which of the following options would be most useful in meeting this requirement?

    a. Utilise the net accounts command to review the shared resources

    b. Utilise the net config command to review the shared resources

    c. Utilise the net file command to review the shared resources

    d. Utilise the net session command to review the shared resources

Answer: Utilise the net file command to review the shared resources

Self Assessment Question

13. ACL stands for Access Control List

a. Access control list

b. Account control list

c. Access configuration list

d. Access control loop

Answer: Access control list

Self Assessment Question

14. The file system NTFS stands for:

a. New type file system

b. Never terminated file system

c. New technology file system

d. Non terminal file system

Answer: New technology file system

Self Assessment Question

15. You organise files by storing them in

a. folders

b. archives

c. indexes

d. lists

Answer: folders

Configuring File and Share Access Permissions

Assignment

1. What things do we consider while making a file share?
2. How do we manage file shares?
3. How can we map drives?
4. What are the basic permissions? How can we assign them?
5. What are advanced and inheriting permissions?
6. Explain about NTFS Authorisation.
7. What is the file server resource manager?
8. Explain file screening. How do we manage its functionality?
9. How can we create file groups?
10. Explain the storage resource management.

Configuring File and Share Access Permissions

Summary

- File sharing is the public or private sharing of computer data or space in a network with various levels of access privilege.
- Depending on your network environment and what you're trying to accomplish there are four ways to set up file sharing
- A network drive is usually a shared folder or computer that is available on a network and makes it easy to access using File Explorer just like a normal hard disk.
- Permissions define the type of access that is granted to a user or group for an object or object property
- In windows a user who creates an object automatically becomes its owner and can set permissions at his or her discretion.
- File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers.

Configuring File and Share Access Permissions

Document Links

Topics	URL	NOTE
Designing a File-Sharing Strategy	https://searchmobilecomputing.techtarget.com/definition/file-sharing https://www.itprotoday.com/strategy/12-commandments-file-sharing https://social.technet.microsoft.com/Forums/windowsserver/en-US/212eabe6-a5e5-4b89-8984-9834c1fb12cc/file-sharing-strategy?forum=winserverfiles https://ieeexplore.ieee.org/document/7799645/	These links will describe the strategy of file sharing
Arranging shares, controlling access and mapping drives.	https://www.thebalancesmb.com/computer-file-management-tips-2948083 https://kb.iu.edu/d/ahrs https://www.ezcomputersolutions.com/blog/best-practices-organizing-business-files/ https://zapier.com/blog/organize-files-folders/ https://support.microsoft.com/en-in/help/325361/how-to-configure-security-for-files-and-folders-on-a-network-in-window	Given Url will describe the arrangement of sharing files and folders, controlling of file/folder access and mapping the windows drives

Configuring File and Share Access Permissions

Document Links

Topics	URL	NOTE
Arranging shares, controlling access and mapping drives. Creating Folder Shares, Assigning Permissions, Understanding the windows Permission Architecture and Basic	https://pureinfotech.com/setup-network-file-sharing-windows-10/ https://www.ficpa.org/content/News/BizTechNews/TechTips/Map-drive-Windows-10.aspx https://www.itprotoday.com/strategy/magic-drive-mapping https://www.laptopmag.com/articles/map-network-drive-windows-10 http://support.microsoft.com/en-in/help/325361/how-to-configure-security-for-files-and-folders-on-a-network-in-window https://pureinfotech.com/setup-network-file-sharing-windows-10/ https://www.ficpa.org/content/News/BizTechNews/TechTips/Map-drive-Windows-10.aspx https://www.itprotoday.com/strategy/magic-drive-mapping https://www.laptopmag.com/articles/map-network-drive-windows-10 https://support.microsoft.com/en-in/help/4026635/windows-map-a-network-drive http://kb.mcgill.ca/?portalid=2&articleid=2659#tab:homeTab:crumb:8:artId:2659:src:article	url will provide the knowledge of arrangement of shares, managing access of files and folders. Students will know to create the shared folder. They will give different permissions of accessing the data and knowledge of permission architectures
Advanced Permissions, Allowing and Denying Permissions, Inheriting Permissions.	http://support.ricoh.com/bb_v1oi/pub_e/oi_view/0001040/0001040590/view/scanner/unv/0059.htm https://websiteforstudents.com/create-shares-everyone-full-access-windows-10-server/ https://answers.microsoft.com/en-us/windows/forum/windows_10-files/give-permissions-to-files-and-folders-in-windows/78ee562c-a21f-4a32-8691-73aac1415373 https://www.ibm.com/support/knowledgecenter/es/SSZJPZ_9.1.0/com.ibm.swg.im.iis.found.admin.common.doc/topics/wsisinst_install_prmssns_grps_win5plus.html https://www.oreilly.com/library/view/windows-server-2003/0321305019/0321305019_ch03lev1sec1.html	Give URL will aware students regarding the advanced and inheriting permissions and how we will allow and deny permissions.

Configuring File and Share Access Permissions

Document Links

Topics	URL	NOTE
Understanding Effective Access, Setting Share Permissions, Understanding NTFS Authorization, Assigning Basic NTFS Permissions	https://espace.cern.ch/winservices-help/NICESecurityAndAntivirus/NICESecurityHowTo/Documents/ACL_helpPage_v1.0.pdf http://www.ntfs.com/ntfs-permissions.htm https://unix.stackexchange.com/questions/79955/how-do-file-permissions-attributes-work-kernel-level-fs-level-or-both https://pcwww.liv.ac.uk/csd/apptest/UnderstandingRights/explain.html https://www.howtogeek.com/72718/how-to-understand-those-confusing-windows-7-fileshare-permissions/ https://sourcedaddy.com/windows-7/inherited-permissions.html https://sourcedaddy.com/windows-7/inherited-permissions.html https://activedirectorypro.com/how-to-view-ntfs-effective-permissions/ https://www.thewindowsclub.com/effective-permissions-tool-windows https://support.microsoft.com/en-in/help/324067/how-to-set-folder-security-for-shared-folders https://www.globalknowledge.com/us-en/resources/resource-library/articles/best-practices-for-share-permissions-in-windows-server-2016/	By the URL students will aware about accessing file and folders effectively. They will know how to share the permissions. NTFS permissions and their basics and how to make authorization to NTFS permissions
Understanding Resource Ownership, Combining Share and NTFS Permissions, Installing File Server Resource Manager	http://www.ntfs.com/ntfs-permissions-precedence.htm https://www.winhelp.us/ntfs-permissions-in-windows.html http://campus.mst.edu/cis/desktop/documentation/pc/win7_x64/permissions/index.htm http://www.ntfs.com/ntfs-permissions-file-folder.htm http://www.ntfs.com/ntfs-permissions-setting.htm https://social.technet.microsoft.com/Forums/office/en-US/c6242159-d15d-417e-91f8-eb19c0da3a35/best-practices-for-basic-ntfs-permissions-on-a-share?forum=winserverfiles	URL will describe the ownership of available resources, combining NTFS and share permissions. It also describe the installation of FSRM

Configuring File and Share Access Permissions

Document Links

Topics	URL	NOTE
Using, creating, changing Quotas, Managing Files with File Screening, Creating File Groups, Creating a File Screen, Creating a File Screen Exception	https://www.itprotoday.com/strategy/take-control-windows-object-ownership-and-inheritance https://www.windowscentral.com/how-take-ownership-files-and-folders-windows-10 http://etutorials.org/Microsoft+Products/microsoft+windows+xp+professional+training+kit/Chapter+9+-+Administering+Shared+Folders/Lesson+3nbspCombining+Shared+Folder+Permissions+and+NTFS+Permissions/ https://www.techrepublic.com/article/configure-it-quick-combining-sharing-and-ntfs-permissions-in-windows-xp/ https://www.novell.com/documentation/storagemanager5/storagemanager_ad_install/data/bgrt6wl.html http://vmwarediary.com/Tutorials/2017/7/17/File-Server-Resource-Manager-Step-by-Step-Guide-for-Windows-Server-2008-R2 https://mizitechinfo.wordpress.com/2013/08/20/step-by-step-manage-file-server-using-fsrm-file-screening-in-windows-server-2012-r2/ https://mizitechinfo.wordpress.com/2013/08/20/step-by-step-manage-file-server-using-fsrm-file-screening-in-windows-server-2012-r2/	The Given links will describe the file screening and its component in depth. Students will aware to create the file groups and creating the file screen exceptions
Creating a File screen Template. Storage Reports Management	http://help.comodo.com/topic-214-1-771-9454-Introduction-to-Comodo-Device-Manager.html http://help.comodo.com/topic-399-1-786-10158-.html https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-file-screen https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-file-screen-exception https://docs.microsoft.com/en-us/windows-server/storage/fsrm/create-file-screen-template https://docs.microsoft.com/en-us/windows-server/storage/fsrm/storage-reports-management https://blog.foldersecurityviewer.com/windows-server-storage-reports-management/	Given URL will show how to create file screen templates and process of storage report management

Configuring File and Share Access Permissions

Video Links

Topics	URL	Note
Designing a File-Sharing Strategy	https://www.youtube.com/watch?v=ecoliBpLcDI https://www.youtube.com/watch?v=uFQhawnWOrI https://www.youtube.com/watch?v=AG10HiIr9kw	Student will aware about file sharing and strategies
Arranging shares, controlling access and mapping drives	https://www.youtube.com/watch?v=L1-EJOTdYgE https://www.youtube.com/watch?v=lt32NIJKEUA https://www.youtube.com/watch?v=GDVQmSpKRWw https://www.youtube.com/watch?v=kjLF-x6rpM4 https://www.youtube.com/watch?v=G6SQJEKCClg https://www.youtube.com/watch?v=tozfMBjwg2Q https://www.youtube.com/watch?v=1DxpBlBVpdY	Students will know the how to arrange the sharing, the accessibility of files and folders. And how to map the drives
Creating Folder Shares, Assigning Permissions, Understanding the windows Permission Architecture and Basic	https://www.youtube.com/watch?v=8z8yW1JHkHc https://www.youtube.com/watch?v=GMzl1ULzWrM https://www.youtube.com/watch?v=37Kx9oiJKTQ https://www.youtube.com/watch?v=Jno-Fbbogxo https://www.youtube.com/watch?v=VizHFrOqpEE https://www.youtube.com/watch?v=CHQ9LxpZJqk https://www.youtube.com/watch?v=RSOEqb_QglA https://www.youtube.com/watch?v=7jhXa-4cfeA	Students will know about the different type of file permissions and there basics

Configuring File and Share Access Permissions

Video Links

Topics	URL	NOTE
Advanced Permissions, Allowing and Denying Permissions, Inheriting Permissions.	https://www.youtube.com/watch?v=H2I3Ar0ZraU https://www.youtube.com/watch?v=S1gOLcWJfDA https://www.youtube.com/watch?v=kZmXil_ps2I https://www.youtube.com/watch?v=ytmYVbMEsGg https://www.youtube.com/watch?v=B9CfezZ7m0w https://www.youtube.com/watch?v=3LnnvbpO9NI https://www.youtube.com/watch?v=OGmGcnFEQiI https://www.youtube.com/watch?v=Q7x1ahVPbWw	They will know about advance permissions, allowing and denying permissions and inhering permissions
Understanding Effective Access, Setting Share Permissions, Understanding NTFS Authorization, Assigning Basic NTFS Permissions	https://www.youtube.com/watch?v=3DS0N3eW0LE https://www.youtube.com/watch?v=VizHFrOqpEE https://www.youtube.com/watch?v=XQNYkUwmV5E https://www.youtube.com/watch?v=GfmkD12ywfw https://www.youtube.com/watch?v=RSOEqb_QglA	URL will describe effective access of files Different types of permissions and their assignment
Understanding Resource Ownership, Combining Share and NTFS Permissions, Installing File Server Resource Manager	https://www.youtube.com/watch?v=YWgDDip5Bqo https://www.youtube.com/watch?v=KX3Ev_MfyPM https://www.youtube.com/watch?v=GfmkD12ywfw https://www.youtube.com/watch?v=F-KwsBIbTDo https://www.youtube.com/watch?v=1IsNI-hvs_g	Student will understand resource ownership, Installation of file server and combining permissions

Configuring File and Share Access Permissions

Video Links

Topics	URL	NOTE
Using, creating, changing Quotas, Managing Files with File Screening, Creating File Groups, Creating a File Screen, Creating a File Screen Exception	https://www.youtube.com/watch?v=kZiUe6HxsmE https://www.youtube.com/watch?v=SB_R-D09XJw https://www.youtube.com/watch?v=oUCMWKhJDTs https://www.youtube.com/watch?v=XMlDWrs1WOY https://www.youtube.com/watch?v=z1Z6hBQXtnY https://www.youtube.com/watch?v=UbRh1mHBL3k https://www.youtube.com/watch?v=vHpO5vLfcM4 https://www.youtube.com/watch?v=SaF0OhJROHc https://www.youtube.com/watch?v=tn0sKxyCgR8	Videos will describe about management of file screening , quota management, creating file groups and file screen exception
Creating a File screen Template. Storage Reports Management	https://www.youtube.com/watch?v=HyKVmumbOrk https://www.youtube.com/watch?v=bsyBkZQ_UfY https://www.youtube.com/watch?v=lRW7rXIgYKg	Videos will describe about how to create the file screen templates and will give idea about Storage report management

Configuring File and Share Access Permissions

E-Bool Links

URL	NOTE
https://www.ebookfrenzy.com/pdf_previews/WinServer2008R2Preview.pdf https://ptgmedia.pearsoncmg.com/images/9780735625051/samplepages/9780735625051.pdf https://the-eye.eu/public/Books/IT%20Various/MICROSOFT.PRESS.WINDOWS.SERVER.2012.R2.POCKET.CONSULTANT.STORAGE.SECURITY.AND.NETWORKING.2014.pdf	These PDF Link will cover the detail study about this unit