

# **6 NTFS PERMISSIONS AND SECURITY SETTING**

- 6.1 Introduction to NTFS Permissions 6.1.1 File Permissions and Folder Permission
- 6.2 Assigning NTFS Permissions and Special Permission
  - 6.2.1 Planning NTFS Permissions6.2.2 Take Ownership of Files
    - 2.2 Take Ownership of Files and Folders
  - 6.2.3 NTFS Permissions Inheritance
- 6.3 Supporting NTFS Permissions 6.3.1 Effects on Copying Files and Folders
  - 6.3.2 Effects on Moving Files and Folders
- 6.4Overview of Security Policy6.4.1Local Security Policy6.4.2Group Policy
- 6.5 Configuring Account Policy
- 6.6 Configuring User Rights
- 6.6 Configuring Security Option
- 6.7 Summary
- 6.8 Exercise

#### **Objectives**

At the end of this chapter students should be able to:

- Identify the NTFS file and folder permissions
- Identify guidelines for planning NTFS permissions
- Assign or modify NTFS permissions
- Explain the concept of take ownership
- Clarify the concept of NTFS Inheritance
- Explain the effect on NTFS permissions when files and folders are copied or moved
- Identify the security policy
- Identify the user rights
- Identify the Security Options

# 6.1 INTRODUCTION TO NTFS PERMISSIONS

New Technology File System or NTFS is file system that provide performance, security, reliability and advanced features that are not be found in FAT files type. Additionally, NTFS also provides an advanced feature which is known as NTFS permission where it is only available on NTFS system.

This permission is very important to the client operating system as it is used to identify which users and groups can gain access to the files and folders. The example of NTFS permission is the file and folder permission.



In discussing this topic, you should clear first with the definition of permission.

Permission is a rule associates with an object (eg. file, folder, folder shared and printer) to control which users can gain access to the object. Typically, the permissions are granted or denied by the object's owner.

# 6.1.1 File Permission and Folder Permission

Standard permissions are permissions that control a broad range of permission. The most popular standard permission is the Full Control. This is what everyone wants, but in reality very few should get. Full control allow the user (that is granted this permission) to do anything to the object.

Standard permission applies to the file and folders. However, both of them have different permission in assigning which user can access the file or folder. Folders have same standard permission as files but Folder has extra standard permission which is "List Folder Contents".

The table below explain the standard NTFS for the file and folder permissions.

NTFS Permissions	For a File - User can	For a Folder – User can
Read	<ul> <li>Read the file</li> <li>View file permissions, attributes and ownership</li> </ul>	<ul> <li>See files and subfolders in the folder</li> <li>View folder permissions and attributes (such as Read-Only, Hidden, Archive, and System).</li> </ul>
Write	<ul> <li>Overwrite the file</li> <li>change file attributes</li> <li>Views file ownership and permissions.</li> </ul>	<ul> <li>Create new files and subfolders within the folder</li> <li>change folder attributes</li> <li>view folder ownership and permissions</li> </ul>
Read & Execute	<ul> <li>Run applications</li> <li>Perform the Read permission</li> </ul>	<ul> <li>Move through folders to reach other files and folders</li> <li>perform Read permission</li> <li>Perform List Folder Contents permission.</li> </ul>
Modify	<ul> <li>Modify and delete the file</li> <li>Perform the Write permissions</li> </ul>	<ul> <li>Delete the folder</li> <li>perform the Write permission</li> </ul>



	Perform the Read & Execute permission	•	Perform the Read & Execute permission
Full Control	<ul> <li>Change permissions and take ownership</li> <li>Perform all NTFS file permissions (Read, Write, Read &amp; Execute and Modify).</li> </ul>	• (	Change permissions, take ownership, and delete subfolders and files Perform all folder permissions (Read, Write, List Folder Contents, Read & Execute and Modify).
List Folder Contents	-	• ; i	See the names of files and subfolders in the folder.

**Table 6-1 NTFS Permissions** 

# 6.2 ASSIGNING NTFS PERMISSIONS AND SPECIAL PERMISSION

You should follow certain guidelines for assigning NTFS permissions. Hence, the next section will discuss how to plan this permission. It is noted that, assigning permissions must be done according to group and user need.

# 6.2.1 Planning NTFS PERMISSION

There are few guidelines that should be followed before you assigning the NTFS permissions:

i. **Group the files into application, data, and home folders** to simplify administration. Centralize home and public folders on a volume that is separate from applications and the operating system.

The benefits of this guideline:

- Assign permissions only to folders, not to individual files.
- Backup is less complex because there is no need to back up application files and all home and public folders are in one location.
- ii. Allow users only the level of access that they require. If a user only needs to read a file, assign the Read permission to his or her user account for the file. This reduces the possibility of users accidentally modifying or deleting important documents and application files.
- iii. Create groups according to the access that the group members require for resources. Then assign the appropriate permissions to the group. Assign permissions to individual user accounts only when necessary.
- iv. Assign the Read & Execute permission to the Users group and the Administrators group when you assign permissions for working with data or application folders, This prevents application files from being accidentally deleted or damaged by users or viruses.

v. Assign the **Read & Execute** permission and the **Write** permission to the **Users** group, and the **Full Control** permission to **OWNER** when assign permissions for **public data folders**. The user who creates a file is by default the creator and owner of the file.

After you create a file, you may grant another user permission to take ownership of the file. The person who takes ownership would then become the owner of the file. If you assign the **Read & Execute** permission and the **Write** permission to the **Users group**, and the **Full Control** permission to **OWNER**, users have the ability to read and modify documents that other users create and the ability to read, modify, and delete the files and folders that they create.

- vi. **Deny permissions** only when it is essential to deny specific access to a specific user account or group.
- vii. Encourage users to assign permissions to the files and folders that they create and educate them about how to do so.



Before you proceed on this lab, make sure that you can **view the Security tab**, follow steps below:

- TIP
- Click Start, and then click Control Panel.
- Click Appearance and Themes, and then click Folder Options.
- On the View tab, under Advanced settings, clear Use simple file sharing [Recommended] check box.

General View	File Types Offline Fil	es	
- Folder vie	ws You can apply the view you are using for this fold Apply to All Folders	(such as Details or Tiles) ler to all folders. Reset All Folders	that
Advanced s	ettings:		
	unch folder windows in a s anaging pairs of Web page Show and manage the page Show both parts and mar Show both parts and mar Show both parts but man emember each folder's view estore previous folder windo now Control Panel in My Co now control Panel in My Co now encrypted or compress now pop-up description for f se simple file sharing (Reco	eparate process s and folders iir as a single file age them individually age as a single file settings ws at logon mputer ed NTFS files in color older and desktop items inmended	
		Restore Defa	aults
	ОК	Cancel /	Apply

#### 6.2.1.1 LAB: Assigning or Modifying Permissions

Users with the **Full Control** permission and the **owners** of files and folders can assign permissions to user accounts and groups. Follow the steps below to assign or modify NTFS permissions for a file or a folder.

- 1. Right-click the file or folders, for which you want to assign permissions (example: folder Client OS), then click Properties.
- 2. Then, click at the Permission for Administrators to assign the permissions. Click OK.

iroup or user names:		
Administrators (COSMOPOL	-F34713\Administra	itors)
😰 lia (COSMOPOI-F34713\lia)	l.	
🕵 SYSTEM		
	Add	<u>R</u> emove
ermissions for Administrators	Allow	Deny
Full Control	1	
Modify	1	
	4	
Read & Execute	~	
Read & Execute List Folder Contents		
Read & Execute List Folder Contents Read	V	
Head & Execute List Folder Contents Read Write		
Head & Execute List Folder Contents Read Write	Y Y	

Figure 6-1 Client OS Properties dialog box

#### 6.2.1.2 LAB: Adding Permission to the New User

Firstly, you need to add new user in order to add permission. You can see the step below:

1. Click the Add button on the Security tab of a file or folder's Properties dialog. ( eg. Client OS folder).

eneral shairig	Security	Customize		
Group or user na	mes:			
Administrat     Administrat     Administrat     Administrat     Sia (COSMC     SYSTEM	ors (COSMC )POI-F3471	)POI-F3471 3\lia)	3\Administra	stors)
Permissions for S	YSTEM		Add	<u>R</u> emove
Full Control	TOTEM		2	
Modify			1	
Read & Execu	ate		14	
	ntents		1	
List Folder Co			1	
List Folder Co Read			121	
List Folder Co Read Write				
List Folder Co Read Write			H	<b>C</b> 1.

Figure 6-2 Adding permission to the new user

2. Select Users or Groups dialog box will appear.

Select Users or Groups	? 🔀
Select this object type:	
Users, Groups, or Built-in security prine	sipals Object Types
From this location:	
DELL	Locations
Enter the object names to select (exam	iples):
r	Check Names
Advanced	OK Cancel

Figure 6-3 The Select Users or Groups appear after you add new user

Figure 6-3 describes about options available in the Select Users or Groups dialog box:

Option	Description
Select This Object Type	Allows you to select the types of objects (eg. groups and computer accounts).
From This Location	Indicates where you are currently looking; for example, in the domain or on the local computer.
Locations	Allows you to select where you want to look; for example, in the domain or on the local computer.
Enter The Object Names To Select	Allows you to type in a list of built-in users or groups to be added.
Check Names	Verifies the selected list of built-in users or groups to be added.
Advanced	Allows you access to advanced search features, including the ability to search for deleted accounts, accounts with passwords that do not expire, and accounts that have not logged on for a certain number of days.

Table 6-2 Select Users or Groups dialog box.



3. Next, insert the object name in **Enter the object names** (e.g razak). Then click **OK** button.

elect Users or Groups	?
Select this object type:	
Users, Groups, or Built-in security pri	ncipals Object Types
From this location:	
DELL	Locations
Enter the object names to select (exa	imples):
razak	Check Names

Figure 6-4 Insert the object name

4. Now, the object name (eg. razak ) become a new user for the group. Then, you can assign permissions this object name.

?
Customize
01-F34713\Administrators) lia)
13\razak
Add Bemove
Allow Deny
idvanced settings, Advanced

Figure 6-5 Permission for the object name (eg. razak)

#### 6.2.1.3 LAB: Grant or Deny Special Permissions

Use following steps to grant or deny the selected user:

1. Click Advanced button.

ieneral Shari	ng Security	Customize		
Group or user	names:			
🚮 Administ	rators (COSMC	DP0I-F34713	Administra	tors)
🖸 lia (COSt	MOPOI-F3471	3\lia)		
🖸 razak (Cl	OSMOPOI-F34	4713\razak)		
SYSTEM	1			
20				Demous
		Ag	<u>90</u>	Temove
Permissions fo	r razak		Allow	Deny
Full Control				
Modify				
Read & Exe	ecute			
List Folder (	Contents		Image: A start of the start	
Read				
Write				
Consist Day	missions			- E
		r advanced s	ettings,	Advanced
For special pe	rmissions of to	0010000		and a second secon
For special pe click Advance	rmissions or to ed.	a davancea a		Multancea

Figure 6-6 Select the Advanced button to grant or deny special permission

2. The Advanced Security Settings for Client OS dialog box will appear which lists the users and groups and the permissions they have on this object.

The **Permissions Entries** box also shows where the permissions were inherited from and where they are applied. To change the permissions set for a user or group, select a user and click **Edit** button.

vanced S emissions To view mo	ecurity Setting Auding Dwner miniomation abou	a for Client OS Ellective Penassons Special permissions, re	dect a permission entry	, and then click Edit.
Pennission Type	oripies: Name	Permission	Inherited From	Acoly To
Allow Allow Allow Allow	nask 8005M0E0 Administrators (809 & (8005M0P0173 SYSTEM	F., Read & Execute M., Full Control 47., Full Control Full Control	Cost inherited Parent Object Parent Object Parent Object	This folder, subfolders This folder, subfolders This folder, subfolders This folder, subfolders
Agti Inheit h defined Reglace	om parent the permi here.	<ul> <li>Berrier</li> <li>Berrier</li> <li>con entries that apply</li> <li>on all child objects with</li> </ul>	e to child objects: Includ entries: shown here that	e these with entries explicitly Il apply to child objects
			OK )	Cancel

Figure 6-7 Select the user that you need to set permission

3. The **Permission Entry for Client OS** dialog box will appear. You can select or clear the specific permissions for that user. Refer the Table 6-3 Special permissions to view the detail in the permissions.

Name: Isazak (COSMOPOLE	34713\razak]	Change.
Apply grito: This folder, subto	iders and files	~
Permissions:	Allow	Deny
Full Control		
Traverse Folder / Execute F	de 🖌	
List Folder / Read Data	1	
Read Attributes	Sec. 1	
Read Extended Attributes	<b>~</b>	
Create Files / Write Data		
Create Folders / Append Da	Ro 🖂	
Write Attributes		
Write Estended Altributes		
Delete Subfolders and Files		
Delete		
Read Permissions	1	
Charas Damiladana	(TT)	— —

Figure 6-8 Select the permission that you want to assign for the user

Table 6-3 explain the special permission that you can change to the user.

Permission	Description
Traverse Folder/ Execute File	<ul><li>Traverse Folder</li><li>Apply only to the folders</li></ul>
	• Allows a user to move (or denies a user from moving) through folders.
	Execute File
	Apply only to the files
	<ul> <li>Allows or denies running executable files (application files). Execute File applies only to files.</li> </ul>
List Folder/	List Folder
Read Data	Allows or denies viewing file names and subfolder names within the folder. List Folder applies only to folders.
	Read Data
	Allows or denies viewing the contents of a file.
	Read Data applies only to files.
Read Attributes	• Allows or denies the viewing of the attributes of a file or folder.
Read Extended Attributes	Allows or denies the viewing of extended attributes of a file or a folder.     These attributes are defined by programs.
Create Files/	Create Files
Write Data	Allows or denies the creation of files within a folder. It applies to
	folders only.
	Write Data
	<ul> <li>Allows or denies the making of changes to a file and the overwriting of existing content.</li> </ul>
Create Folders/	Create Folders
Append Data	<ul> <li>Allows or denies the creation of folders within the folder. It applies only to folders.</li> </ul>

	<ul> <li>Append Data</li> <li>Allows or denies making changes to the end of the file (not included changing, deleting, or overwriting existing data).</li> </ul>
Write Attributes	• Allows or denies the changing of the attributes of a file or folder.
Write Extended Attributes	• Allows or denies the changing of the extended attributes of a file or a folder. These attributes are defined by programs.
Delete Subfolders And Files	Allows or denies the deletion of subfolders or files within a folder.
Delete	Allows or denies the deletion of a file or folder.
Read Permissions	Allows or denies the Read permissions that are assigned to the file or folder.
Change Permissions	Allows or denies the Change Permission that is assigned to the file or folder.
Take Ownership	Allows or denies taking ownership of the file or folder.
Synchronize	• Allows or denies different threads in a multithreaded program to synchronize with one another.
	A multithreaded program performs multiple actions simultaneously by using both processors in a dual-processor computer.

**Table 6-3 Special permissions** 

# 6.2.1.4 LAB: Remove Existing User

NTFS Permission also allows you to remove an existing user. Follow the steps below.

1. Highlight the user name that you want to remove. Then, click Remove button.

Seneral Sharing Security	Customize
Enoup or user names:	
diministrators (COSMOP	OI-F34713\Administrators)
1 ka (COSMOPOLF34713)	dia)
S Incal (COSMOPOLE347	13vazak)
SYSTEM	
	-
	Add. Bemove
Eemissions for sazak	Allow Dery
Full Control	
Modily	
Read & Execute	
List Folder Contents	
Read	
Write	
Courses Onuitations	F F 🕷
For special permissions or for a click Advanced.	advanced sellings. Advanced

Figure 6-9 Removing the existing user

# 6.2.2 Take Ownership of Files and Folders

Every object (file or folder) on an NTFS volume has an owner who controls how permissions are set on the object and to whom permissions are granted. When a user creates an object, that user automatically becomes the object's owner.

The owner of a file, an administrator, or anyone with Full Control permission can assign Take Ownership permission to a user account or group, allowing them to take ownership.

The following rules apply for taking ownership of a file or folder:

- i. The **current owner** or any user with **Full Control** permission can assign the Full Control standard permission or the Take Ownership special access permission to another user account or group, allowing the user account or any member of the group to take ownership.
- ii. An **administrator** can take ownership of a folder or file. If an administrator takes ownership, the Administrators group becomes the owner, and any member of the Administrators group can change the permissions for the file or folder and assign the Take Ownership permission to another user account or group.



If an employee leaves the company, an administrator can take ownership of the employee's files and assign the Take Ownership permission to another employee, and then that employee can take ownership of the former employee's files.

#### 6.2.2.1 LAB: Take Ownership of Files and Folders

Take ownership of a file or folder can be done by follow the steps below:

1. In the Security tab of the Properties dialog box for the file or folder, click Advanced.

ieneral Sharing Security Cust	xenize	
Group or user names:		
Administrators (COSMOPOL4	34713VAdministra	fors]
Ia (COSMOPOI-F34713\la)		
I razak (COSMOPOI-F34713V	(azak)	
SYSTEM		
	Add	Bemove
Bermissions for Administrators	Allow	Deny
Full Control	12	
Modify	(# <sup>2</sup> )	
Read & Execute	1	
List Folder Contents	1	
Read		
White	-	
Convid Documentary		- m - M
For special permissions or for adva click Advanced.	nced settings.	Advanced

Figure 6-10 Use Advance button to set special permission

6

2. In the Advanced Security Settings button, in the Owner tab, in the Change Owner To list, select your name.

Select the **Replace owner on subcontainers and objects** check box to take ownership of all subfolders and files that are contained within the folder, and then click **Apply** and **OK** buttons.

STREET INTE	Auditing Dwmer	Effective Permission			
rieu can tak	e ownership of an	object if you have the	appropriate permiss	iona.	
Current overs	e of this iters:				
la (COSMO)	POI-F34713Vila)				
hange gwn	er ta:				
Name					-
1 la(CO	Maton (CUSMUP SMDPOLF34713V	la)	onij		
1 ka (CO)	Materi (JUSMOP MOPOLF34713)	(ar (ar i ) waanaang	out		

Figure 6-11 Use the Owner tab of the Advance Security Settings to take ownership

# 6.2.3 NTFS Permissions Inheritance

By default, the permission that you assign to the parent folder are inherited to the subfolders and files contained in the parent folder (Figure 6-12).



**Figure 6-12 Inherit permissions** 

However, you can prevent this inheritance. It means that the default inheritance can be changed. This makes the subfolders and files to not inherit permissions that have been assigned to the parent folder (Figure 6-13).





Figure 6-13 Prevent inheritance

#### 6.2.3.1 LAB: Prevent Permissions Inheritance

By default, the subfolders and files inherit permissions that you assign to their parent folder. Use following steps to prevent permissions inheritance:

1. In Security tab, Click Advanced button.

contrar a strate of a second of	lustomize	
proup or user names:		
Administrations (DOSMOPH     Second Cost (DOSMOPH)     Second Cos	06434713%Adminisha ia) 13Yaazak)	fors)
	Add.	Bessove
enmissione for Administrations	Allow	Deny
Full Control	21	
Modily	14	
Read & Execute	198	
List Folder Contents		
Read		
10000	$\neg P$	
Wile		

Figure 6-14 The Advanced button of the Security tab allow you to prevent permissions inheritance

2. The Advanced Security Settings dialog box will appear. In preventing a subfolder or file from inheriting permissions from a parent folder, clear the Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here check box.

o view m	ore information about Spe	cial permissione, se	elect a permission entry.	and then click Edit.
ermission	rențsies:			
Type	Name	Pennission	Inherited From	Apply To
Allow	sazak (COSMOPOLF	Modily	(not inherited)	This folder, subfolders
Allow.	lia (COSMOPO#F347	Full Control	C:\Documents a	This folder, subfolders
Allow	SYSTEM	Full Control	C:\Decuments a	This folder, subfolders
Allow	Administrations (CUSM	Full Control	L'ADiocuments a	This forcer, subroiders
Ad	4	Beno	~	
	how parent the permission there.	entries that apply	to child objects. Include	these with entries explicitly
Inherit				
nhent define	e permission entries on all	child objects with	entries shown here that	apply to child objects
] Inherit definer ] Reglac	e pesnission entries on all	child objects with	entries shown here that	apply to child objects

Figure 6-15 Clear the Inherit from parent permission entries to prevent file from inheriting permissions from a parent folder

3. Security dialog box will appear. You are then prompted to select one of the options (Copy, Remove or Cancel). These options described inTable 6-4.



Figure 6-16 Option in the permission

Option	Description
Сору	<ul> <li>Copy the permission entries that were previously applied from the parent to the child.</li> <li>deny subsequent permissions inheritance from the parent folder.</li> </ul>
Remove	• Remove the permission entries that were previously applied from the parent to the child.
Cancel	Cancel the permission entries.

Table 6-4 Options in Security dialog box to prevent permissions inheritance

# **6.3 SUPPORTING NTFS PERMISSIONS**

A problem might also arise while you assign or modify NTFS permissions to the files and folders. In this case, the NTFS permissions that you set sometimes change as the file and folders are moved or copied.

Thus, this section discusses the effect on NTFS file and folder permissions when files and folders are copied. This section also discuses the effect on NTFS file and folder permissions when files and folders are moved.

# **6.3.1 Effects on Copying Files and Folders**

Permissions change when you copy files or folders from one folder to another or from one volume to another. For example, if you copy folders to the FAT volumes, the folders will lose their NTFS permissions. This is because the FAT system did not support NTFS permissions.



Figure 6-17 Copying files and folders

When you copy a file within or between NTFS volumes, note the following:

- i. Windows XP Professional treats it as a new file. As a new file, it takes on the permissions of the destination folder.
- ii. You must have Write permission for the destination folder to copy files and folders.
- iii. You become the creator and owner.

# <u>COSMOPOÁNT</u>

# **6.3.2 Effects on Moving Files and Folders**



Permissions also might or might not change when you move a file or folder.

Figure 6-18 Moving files and folders

When you move a file or folder within NTFS volume:

- i. The file or folder retains the original permissions.
- ii. You must have the **Write** permission for the destination folder to move files and folders into it.
- iii. You must have the **Modify** permission for the source file or folder. The **Modify** permission is required to move a file or folder because Windows 2000 deletes the file or folder from the source folder after it is copied to the destination folder.
- iv. You become the creator and owner.

When you move a file or folder between NTFS volumes:

- i. The file or folder inherits the permissions of the destination folder.
- ii. You must have the **Write** permission for the destination folder to move files andfolders into it.
- iii. You must have the **Modify** permission for the source file or folder. The Modify permission is required to move a file or folder because Windows XP Professional deletes the file or folder from the source folder after it is copied to the destination folder.
- iv. You become the creator and owner.

# 6.4 OVERVIEW OF SECURITY POLICY

A security policy means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

Security Policy in Windows XP Professional refers to two types of policies:

• Local Security Policy

This policy is applied to specific computers that are members of a workgroup.

• Group Policy

Group Policy is applied to sites, domains, and it affects all computers or users that are members of the container to which the Group Policy is assigned.

# 6.4.1 Local Security Policy

Local Security Policy allow you to implement security-relevant settings on a local computer such as group membership, permissions and rights, password requirements, desktop settings, and much more. For computers in a workgroup environment, Local Security Policy offers a way to apply consistent restrictions across those computers.

The security settings in Local Security Policy are:

- Account policies this includes password policies, such as minimum password length and account lockout settings.
- Local policies this includes audit policy, user rights and security options.
- **Public key policies** it is used to configure encrypted data recovery agents and trusted certificate authorities.
- Software restriction policies it is used to prevent unwanted applications
- IP security policies it is used to configure the security of network Internet protocol
- System services it is used to manage security setting such as network services, file and print services and Internet services.
- **Registry** this is used to manage the security on Registry subkeys and entries.
- File system this is used to manage the security settings on the local file system.

# 6.4.2 Group policy

One of the most powerful aspects of Windows XP Professional is the implementation of Group Policy. Group Policy is the administrator's primary tool for defining and controlling how programs, network resources, and the operating system behave for users and computers in an organization. This policy can either be configured at the local level or within the Active Directory structure.

<u>COSMOPOÅNT</u>

In an Active Directory environment, this policy is applied to users or computers on their membership in sites, domains, or organizational units. Regardless of the location of implementation, this setting can change the way normal control and administration is done within a company.

Administrators can manage the Group Policy components listed in the Table 6-5 below.

Component	Description
Enforce password history	The system can remember a specified number of previous passwords. When a user attempts to change his password, the new password is compared against the history; if the new is unique, the change is allowed.
Administrative Templates	Set registry-based policy.
Security Settings	Configure security for domains, computers and users.
Software Installation	Assigns or publishes programs
Scripts	Specify scripts for user logon and logoff and computer startup and shutdown.
Folder Redirection	Places special folders, such as My Documents, on the network

**Table 6-5 Group Policy Components** 

# 6.5 CONFIGURING ACCOUNT POLICY

Account policy is a policy that controls the password requirements and how the system responds to invalid logon attempts. There are two types that you can configure in this policy: Password Policy and Account Lockout Policy. Both of them are useful to improve the security on your computer (Refer Figure 6-19 and Figure 6-19 to see the screenshots).

📴 Local Security Settings		
File       Action       View       Help            ← →          ←          ←          ⊕            ⊕ Security Settings           ⊕          ⊕          ⊕            ⊕ Security Settings           ⊕          ⊕          ⊕          ⊕            ⊕ Security Settings           ⊕          ⊕          ⊕          ⊕          ⊕            ⊕ Security Settings           ⊕	Policy / Enforce password history Maximum password age Minimum password age Minimum password length Password must meet complexity re Store password using reversible e	Security Setting O passwords remem 42 days O days O characters Disabled Disabled

Figure 6-19 Password policy in Account Policies



🝺 Local Security Settings		
File Action View Help ← →  € × ⊕	[p.t.	
Image: Count Policies         Image: Count Policies <td< td=""><td>Policy / Account lockout duration Reset account lockout threshold Reset account lockout counter after</td><td>Security Setting Not Applicable 0 invalid logon atte Not Applicable</td></td<>	Policy / Account lockout duration Reset account lockout threshold Reset account lockout counter after	Security Setting Not Applicable 0 invalid logon atte Not Applicable

Figure 6-20 Account Lockout Policy in Account Policies

You can specify the account policy such as following:

Setting	Description
Enforce password history	The system can remember a specified number of previous passwords. When a user attempts to change his password, the new password is compared against the history; if the new is unique, the change is allowed.
Maximum password age	specifies the period of time after which a password must be changed
Minimum password length	Specifies the number of characters in a password. Most passwords should not exceed 14 characters.
Passwords must meet complexity requirements	This policy does not allow a password change unless the new password contains at least three of four character types: uppercase (A through Z), lowercase (a through z), numeric (0 through 9) and non-alphanumeric (such as!).
Store password Using Reversible Encryption For all users in the domain	This policy enables to store reversibly encrypted password for all users in the domain.
Account lockout duration	Specifies how long logon attempts are denied after a lockout.
Account lockout threshold	Specifies the number of denied logon attempts after which an account is locked out.
	For example, if this is set to 3, a lockout occurs if a user enters the wrong password three times; any further logon attempts will be denied.
Reset Account Lockout counter After	Specifies the number of minutes after which the counter that applies to the lockout threshold is reset.
	For example, if the counter is reset after five minutes and the account lockout threshold is three, a user can log on twice with the incorrect password. After five minutes, the counter is reset, so the user can log on twice more. A third invalid logon during a five-minute period lock out the counter.

**Table 6-6 Account Policy settings** 

#### 6.5.1.1 LAB: Changing the passwords setting

Local security policy can be modified by using the Local Security Policy console. Follow the steps below:

- 1. Click start, click Control Panel and then click Administrative Tool.
- 2. In the Administrative Tools, double click Local Security Policy.



Figure 6-21 The security setting in the Local Security Policy

3. In the Local Security Policy window, select policy which needs to edit. For example the Password Policy. In this case, you want to change setting for password length.



Figure 6-22 The Local Security Policy views available policies and current settings

4. In the right pane, double click the policy. Then configure the settings for the policy and click OK.

# <u>соѕморојит</u>

Minimum password length Properties		
Local Security Setting		
Minimum password length		
Password must be at least: 8		
OK Cancel Apply		

Figure 6-23 Change the settings for the Password Policy

#### 6.6 **CONFIGURING USER RIGHT**

Administrators can assign specific rights to group accounts or to the individual user accounts. These rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories.

Each user rights allow the members of the group or individual users assigned the right to perform certain tasks. In assigning user rights, it is recommended that it should be assigned only to groups, not to individual user accounts. This is to simplify the task of user account administration.

There are two types of user rights: Privilege and logon rights.

Privileges	Logon rights
A privilege is a user right that allows the	A logon right is a user right to a group or individual
group members to which it is assigned to	user account.
perform a specific task (eg. the right to back	
up files and directories).	It controls the way users logging to a system such as
	the right to log on to a system locally.

#### **Table 6-7 Privilege and Logon Rights**

6

The following is a list of rights available within the User Right assignment:

Privileges	Logon rights
<ul> <li>Act as part of operating system</li> <li>Add workstations to domain</li> <li>Adjust memory quotas for a process</li> <li>Backup files and directories</li> <li>Bypass traverse checking</li> <li>Change the system time</li> <li>Create a pagefile</li> <li>Debug programs</li> <li>Enable computer and user accounts to be trusted for delegation</li> <li>Force Shutdown from a remote system</li> <li>Load and unload device drivers</li> <li>Manage auditing and security log</li> <li>Modify system environment</li> <li>Perform volume maintenance tasks</li> <li>profile single process to monitor performance of nonsystem processes</li> <li>profile system performance</li> <li>remove computer from docking station</li> <li>restore file and directories</li> <li>shut down the system</li> </ul>	<ul> <li>access this computer from the network</li> <li>Deny access to this computer from the network</li> <li>Logon as batch job</li> <li>Deny logon as a batch job</li> <li>Log as a service</li> <li>Deny logon as a service</li> <li>logon locally</li> <li>Deny logon locally</li> <li>Allow logon through Terminal Services</li> <li>Deny logon through Terminal Services</li> </ul>

Table 6-8 Assigning User rights

# 6.7 CONFIGURING SECURITY OPTIONS

Window XP Professional offers an additional security options in order to keep the computer secure and to define more control over the computer.

Such security options are grouped into the following categories: accounts, audit, devices, domain controller, domain member, interactive logon, Microsoft network client, network access, network security, recovery console, shutdown, system cryptography, and system objects.

The security options can be accessed in the Local Security window, which it is inside the Local Policies Folder. The screenshot of Security Options is viewed in Figure 6-24.

# 6



File Action View Help			
Security Settings	Policy /	Security Setting	
Account Policies     Account Policies     Account Policies     Security Options     Public Key Policies     Software Restriction Policies     IP Security Policies on Local Computer	Accounts: Administrator account status Accounts: Guest account status Accounts: Guest account use of blank p., Accounts: Rename administrator account Accounts: Rename duest account Accounts: Rename guest account Audit: Audit the use of Bockup and Restore Audit: Shut down system immediately F una DCOM: Machine Access Restrictions in Secu Devices: Alowed to format and elect remov Devices: Alowed to format and elect remov Devices: Alowed to format and elect remov Devices: Restrict CD-ROM access to locally l Devices: Restrict ficppy access to locally l	Enabled Enabled Administrator Guest Disabled Disabled Disabled Not defined Enabled Administrators Disabled Disabled Disabled Disabled Disabled	

**Figure 6-24 Security Options** 

### 6.7.1.1 LAB: Configuring Security Settings

In this lab, you configure the security settings that automatically rename the Guest account on your computer.

- 1. Log on with an account that is a member of the Administrators group.
- 2. Click Start, and then click Control Panel., click Administrative Tools
- 3. In the Administrative Tools window, double-click Local Security Policy.
- 4. In the Local Security Settings window, expand Local Policies, and then click Security Options.
- 5. In the right-hand pane, right-click Accounts: Rename Guest Account, and then click Properties.

Local Security Settings				
File Action Wew Help				
⇔ → 💼 × 🗗 🖫 😢				
Security Settings	Policy /	Security Setting		*
Account Policies     Audit Policy     Audit Policy     Audit Policy     Audit Policy     Socurity Options     Socurity Options     Software Restriction Policies     Software Restriction Policies     Descurity Policies on Local Computer	Accounts: Administrator accou     Accounts: Guest account statu     Accounts: Linut local account u     Accounts: Linut local account u     Accounts: Rename administrat	nt s Enabled s Enabled se o Enabled or a Administrator		
	Accounts: Rename quest acco	int Guest	Properties	
	Auck: Audit the use of Backup	an Disabled	Help	
	Audit: Shut down system imme	dist Disabled		
	DCOM: Machine Access Restric	tion Not defined		
	Devices: Alow undick without	hav Enabled		

Figure 6-25 Click the Properties to configure the security settings

6. In the Accounts: Rename Guest Account Properties dialog box, type Fox, and then click OK. Close the Local Security Settings window.

File Action View Help			
⇔ → 🖻 🗡 🗃 🖳 🔗			
<ul> <li>Security Settings</li> <li>Account Policies</li> <li>Audit Policy</li> <li>Guser Rights Assignment</li> <li>Security Options</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Software Policies on Local Computer</li> </ul>	Policy / Accounts: Administrator account s Accounts: Guest account status Accounts: Limit local account use o Accounts: Rename administrator a Accounts: Rename guest account Audit: Audit the access of global s Audit: Audit the use of Backup an Audit: Audit the use of Backup an Audit: Shut down system immediat DCOM: Machine Access Restriction DCOM: Machine Launch Restrictio Devices: Allow undock without hav	Security Setting Enabled Enabled Administrator Fox Disabled Disabled Disabled Not defined Not defined Enabled	



- 7. Click Start, and then click Control Panel.
- 8. In the Control Panel window, click User Accounts.
- 9. What is the name of the Guest account?



Figure 6-27 the user account display Guest Account "Fox"

10. Close the User Accounts window and the Control Panel window.





- 1. NTFS permission is used to identify which users and groups can gain access to the files and folders.
- 2. NTFS folder permissions are Read, Write, Read & Execute, Modify Full Control and List Folder Contents.
- 3. NTFS file permissions are Read, Write, Read & Execute, Modify, and Full Control.
- 4. Every object (file or folder) on an NTFS volume has an owner who controls how permissions are set on the object and to whom permissions are granted. When a user creates an object, that user automatically becomes the object's owner.
- 5. The current owner or any user with Full Control permission can assign the Full Control standard permission or the Take Ownership special access permission to another user account or group.
- 6. When you move a file or folder between NTFS volumes, the file or folder inherits the permissions of the destination folder.
- 7. By default, permissions that you assign to the parent folder are inherited by and propagated to the subfolders and files contained in the parent folder. However, you can prevent permissions inheritance.
- 8. When you copy or move files and folders, the permissions you set on the files or folders might change. When you copy files or folders from one folder to another or from one volume to another, the object takes on the permissions of the destination folder. You must have Write permission for the destination folder to copy files and folders.
- 9. Local Security Policy is applied to specific computers that are members of a workgroup.
- 10. Group Policy is applied to sites, domains, and it affects all computers or users that are members of the container to which the Group Policy is assigned.
- 11. Account policy is a policy that controls the password requirements and how the system responds to invalid logon attempts.
- 12. Window XP Professional offers an additional security options in order to keep the computer secure and to define more control over the computer.



#### **True or False**

1.	NTFS permissions can be used on all file systems available with Windows XP Professional.	True □	False □
2.	Only the administrator with Full Control permissions can assign NTFS Permission to users and group to control access to the files and folders.	True □	False □
3.	Read, Write, Read & Execute, Modify and Full Control is the NTFS File Permissions.	True □	False □
4.	File permission can be assigned to the users to control access the folders.	True □	False □
5.	By default, files and folders inherit permissions from their parent folders.	True 🗆	False □
6.	Read folder permissions allow you to delete the folder.	True □	False □
7.	Group Policy is applied to specific computers that are members of a workgroup.	True □	False □
8.	A logon right is a user right to a group or individual user account.	True □	False □
9.	Account policy is a policy that controls the password requirements and how the system responds to invalid logon attempts.	True □	False □
10.	Privilege controls the way users logging to a system such as the right to log on to a system locally.	True 🗆	False □



#### Fill in the Blanks

- 1. \_\_\_\_\_ is used to specify which users and groups can access files and folders.
- 2. The NTFS file permissions are
- 3. \_\_\_\_\_ permissions can view the files attributes, ownership and permissions.
- 4. \_\_\_\_\_ applies all permissions to the user or group.
- 5.  $\underline{}$  allow the members of the group to which it is assigned to perform a specific task.

#### **Multiple Choice Questions**

- 1. Which of the following statements correctly describe NTFS file and folder permissions?
  - A. NTFS specify which users can gain access to the files and folders.
  - B. Only NTFS volume can performs he NTFS permissions.
  - C. NTFS security is effective when users gain access to the files and folders on the local computer.
  - D. NTFS file and folders permissions are Read, Write, Read & Execute, Modify and Full Control.
- 2. Which of the following users or groups can assign permissions to user accounts and groups? Choose all that apply.
  - A. Administrators
  - B. Permissions
  - C. Users with Full Control permission
  - D. Owners of files and folders
- 3. Which of the following correctly describe take ownership of files and folders? Choose all that apply.
  - A. The file owner, an administrator or users with Full Control permissions can assign the Take Ownership permissions.
  - B. Permissions every file and folders on an NTFS volume has an owner who controls how permissions are set on the file and folders and to whom permissions are granted.
  - C. Take ownership is suitable to be applied when employee leaves the company.
  - D. When a user creates a file, that user automatically becomes the file's owner.

- 4. What are your opinions to describe about user rights? Choose all that apply.
  - A. The system time can be changed if you have logon rights.
  - B. All users can assign specific rights to group or individual user accounts.
  - C. There are two types of user rights: privilege and logon rights.
  - D. It is recommended that you assign user rights only to groups, not to the individual user accounts.
- 5. What can be done by account policy? Choose all that apply.
  - A. Allow or deny through the Terminal Services.
  - B. Shut down the computer.
  - C. Enforce password history.
  - D. Specifies how long logon attempts are denied after a lockout.

#### **Subjective Questions**

- 1. Define between file permission and folder permissions?
- 2. What are the permissions for the folder permissions?
- 3. By default, what inherits the permissions that you assign to the parent folder?
- 4. Based on the exercise below, apply your skill on configuring NTFS permission.
  - a) Planning and Assigning NTFS Permissions
  - b) Determining the Default NTFS Permissions for a Folder
  - c) Testing the Folder Permissions for the Exercise Folder
  - d) Assigning NTFS Permissions
  - e) Taking Ownership of a File

#### a) Planning and Assigning NTFS Permissions

1. Log on with an account that is a member of the **Administrators** group and create the **Limited** users listed in the following table.

User Account	Туре
User1	Limited
User2	Limited

- 2. Create the following folders:
  - C:\Exercise



#### b) Determining the Default NTFS Permissions for a Folder

In this exercise, you determine the **default NTFS permissions** for the newly created **Exercise** folder located on a computer running Windows XP Professional in a workgroup environment.

- 1. Log on with a user account that is a member of the Administrators group.
- 2. On the Start menu, right-click My Computer, and then click Explore.
- 3. Expand Local Disk (C:), right-click the Exercise folder, and then click Properties.
- 4. In the **Exercise Properties** dialog box, on the **Security** tab, note the default groups and users that have permissions for the **Exercise** folder.
- 5. Click each user and group in the **Group or user names** list, note the default permissions assigned to each.
- 6. What are the existing folder permissions?
- 7. Click **OK** to close the **Exercise Properties** dialog box.
- 8. Close Windows Explorer and log off.

#### c) Testing the Folder Permissions for the Exercise Folder

- 1. Log on as User1, and then start Windows Explorer.
- 2. Expand the Exercise folder.
- 3. In the **Exercise** folder, create a text document named **Exercise1** and type in the following text: The first four letters in the alphabet are **a**, **b**, **c**, **and d**.
- 4. Were you successful? Why or why not?
- 5. Attempt to perform the following tasks for the file that you just created:
  - Open the file
  - Modify the file
  - Delete the file
- 6. Were you able to complete all of these tasks and why?
- 7. In the Exercise folder, re-create the text file named Exercise1.
- 8. Log off Windows XP Professional.
- 9. Log on as **User2** and attempt to perform the following tasks on the **Exercise1** text document:
  - Open the file
  - Modify the file
  - Delete the file
- 10. Which tasks were you able to perform and why?

6

#### d) Assigning NTFS Permissions

In this exercise, you assign **NTFS permissions** for the **Exercise** folder. The permissions that you assign are to be based on the following criteria:

- All users should be able to **read** documents and files in the **Exercise** folder.
- All users should be able to **create** documents in the **Exercise** folder.
- All users should be able to modify the contents, properties, and permissions of the documents that they create in the Exercise folder.
- User2 is responsible for maintaining the Exercise folder and should be able to modify and delete all files in the Exercise folder.
- 1. What changes in permission assignments do you need to make to meet each of these four criteria? Why?
- 2. You are currently logged on as **User2**. Can you change the permissions assigned to **User2** while logged on as **User2**? Why or why not?
- 3. Log on with a user account that is a member of the Administrators group, and then start Windows Explorer.
- 4. Expand the **Exercise** folder.
- 5. Right-click the Exercise folder and then click Properties.
- 6. In the Properties dialog box for the folder, on the Security tab, click Add.
- 7. In the Select Users or Groups dialog box, in the Enter the object names to select text box, type User2, and then click Check Names.
- 8. *Computer\_name*\User2 should now appear in the **Enter the object names to select** text box, indicating that Windows XP Professional located **User2** on the computer and it is a valid user account. Click **OK** to close the **Select Users or Groups** dialog box.
- 9. User2 now appears in the Group or user names box in the Exercise Properties dialog box. Click User2 and note the assigned permissions.
- 10. Which permissions are assigned to User2?
- 11. Click Advanced.
- 12. In the Advanced Security Settings for Exercise dialog box, ensure that User2 is selected, and then click Edit.
- 13. In the **Permission Entry for Exercise** dialog box (with User2 displayed in the **Name** text box), in the **Allow** column, click **Full Control**.
- 14. Click OK to close the Permission Entry for Exercise dialog box.
- 15. Click OK to close the Advanced Security Settings for Exercise dialog box.
- 16. Click **OK** to close the **Exercise Properties** dialog box.
- 17. Close Explorer and log off Windows XP Professional.

#### e) Taking Ownership of a File

In this exercise, you observe the effects of taking ownership of a file. To do this, you must determine permissions for a file, assign the Take Ownership permission to a user account, and then take ownership as that user.

To determine the permissions for a file:

- 1. Log on with a user account that is a member of the **Administrators** group, and then start **Windows Explorer.**
- 2. Open Exercise folder.
- 3. Right-click Exercise in Exercise folder and then click Properties.
- 4. In the **Exercise Properties** dialog box, click the **Security** tab. Note the permissions for the **Exercise** file.
- 5. Click Advanced.
- 6. In the Advanced Security Settings for Exercise1 dialog box, on the Owner tab, note the current owner of the file.
- 7. Who is the current owner of the Exercise1 file?\_\_\_\_\_

To assign permission to a user to take ownership:

- 1. In the Advanced Security Settings for Exercise dialog box, on the Permissions tab, click Add.
- 2. In the Select User or Group dialog box, in the Enter the object name to select text box, type User1, and then click Check Names.
- 3. User1 should now appear in the Enter the object name to select text box, indicating that Windows XP Professional located User1 on the computer and it is a valid user account. Click OK.
- 4. In the **Permission Entry for Exercise** dialog box, notice that all the permission entries for **User1** are blank.
- 5. Under **Permissions**, select the **Allow** check box next to **Take Ownership**, and then click **OK**.
- 6. In the Advanced Security Settings for Exercise1 dialog box, click OK to return to the Exercise1 Properties dialog box.
- 7. Click **OK** to apply your changes and close the **Exercise1 Properties** dialog box. Close **Windows Explorer**, and then **log off** Windows XP Professional.

To take ownership of a file:

- 1. Log on as User1, and then start Windows Explorer.
- 2. Select the Exercise folder.
- 3. Right-click Exercise1 and then click Properties.
- 4. In the Exercise1 Properties dialog box, on the Security tab click Advanced.
- 5. In the Advanced Security Settings for Exercise1 dialog box, on the Owner tab, in the Change Owner To list, select User1, and then click Apply.
- 6. Who is now the owner of the **OWNER** file?
- 7. Click OK to close the Advanced Security Settings for Exercise1 dialog box.
- 8. Click **OK** to close the **Exercise1 Properties** dialog box.