Setting Access Controls on Files, Folders, Shares, and Other System Objects in Windows 2000

- Define and set DAC policy (define group membership, set default DAC attributes, set DAC on files systems)

- Modify DAC access control attributes (FMT_MSA.1(a))

- Revoke security attributes associated with objects (FMT_REV.1(b))

On This Page

Key Concepts
Copying vs. Moving
File Permissions
Folder permissions
Selecting where to apply permissions
Setting or modifying permissions
How inheritance affects file and folder permissions
Shared folder permissions
Active Directory object permissions
Setting printer security permissions and shares

Key Concepts

Access control is the process of authorizing users and groups to access objects on the network. Key concepts that make up access control are described below.

- **Least Privilege Principle:** A key component of authorization is the least privilege principle, which states that all users should have the least possible amount of systems access that still allows them to perform their job functions. Thus, if a user only needs to be able to view a particular file, that user should have read-only access to the file; the user should not be able to write to that file.

- **Ownership of Objects:** Windows 2000 assigns an owner to an object when the object is created. By default, the owner is the creator of the object.

- **Permissions Attached to Objects:** The primary means for access control is permissions, or access rights. In Windows systems, permissions can be set on files, folders, and other objects within the system. Permissions allow or deny users and groups particular actions for users and groups. Permissions are implemented primarily by way of security descriptors, which also define auditing and ownership. An example of a permission attached to an object is Read permission on a file. When first installing a Windows system, make sure system object permissions are properly set. In some cases, the system defaults to least privilege; in other cases it may not. Determining whether system permissions conform to the least privilege principle, and modifying those which do not, is called hardening the operating system. This should be done as part of the initial system installation process (See the Windows 2000 Security Configuration Guide for the permission that must be placed on certain objects to meet the Windows 2000 ST).

- **Inheritance of permissions:** Windows 2000 provides a feature for administrators to easily assign and manage permissions. Known as inheritance, this feature automatically causes objects within a container to inherit the permissions of that container. For example, the files within a folder, when created, inherit the permissions of the folder.

- **Object managers:** If there is a need to change the permissions on an individual object, the appropriate tool must be used to change the properties for that object. For example, to change the permissions on a file, start Windows

Explorer, right-click on the file name, and click **Properties**. This dialog box can be used to change permissions on the file.

- **Object auditing:** Windows 2000 allows the administrator to audit users' access to objects. These security-related events can be viewed in the security log with the Event Viewer.

Top Of Page

Copying vs. Moving

When using NTFS permissions to secure access to specific files or folders, it is very important to pay close attention to what happens to those permissions whenever the object is moved or copied to another location on the system.

- When an object is copied into another directory it inherits the access privileges in place at the destination folder.
- When a file or directory object is moved from one directory to another directory, the NTFS permissions that have been applied to the file move with it.

Top Of Page

File Permissions

File permissions include Full Control, Modify, Read & Execute, Read, and Write. Each of these permissions consists of a logical group of special permissions. The following table lists NTFS file permissions and specifies which special permissions are associated with that permission.

NTFS File Permissions

Special Permissions	**Full Control**	**Modify**	**Read & Execute**	**Read**	**Write**
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	✓				
Take Ownership	✓				

Synchronize	✓	✓	✓	✓	✓

Warning: Groups or users granted Full Control on a folder can delete any files in that folder regardless of the permissions protecting the file.

Top Of Page

Folder permissions

Folder permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Each of these permissions consists of a logical group of special permissions. The following table lists NTFS folder permission and specifies which special permissions are associated with that permission.

Folder Permissions

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
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	✓					
Take Ownership	✓					

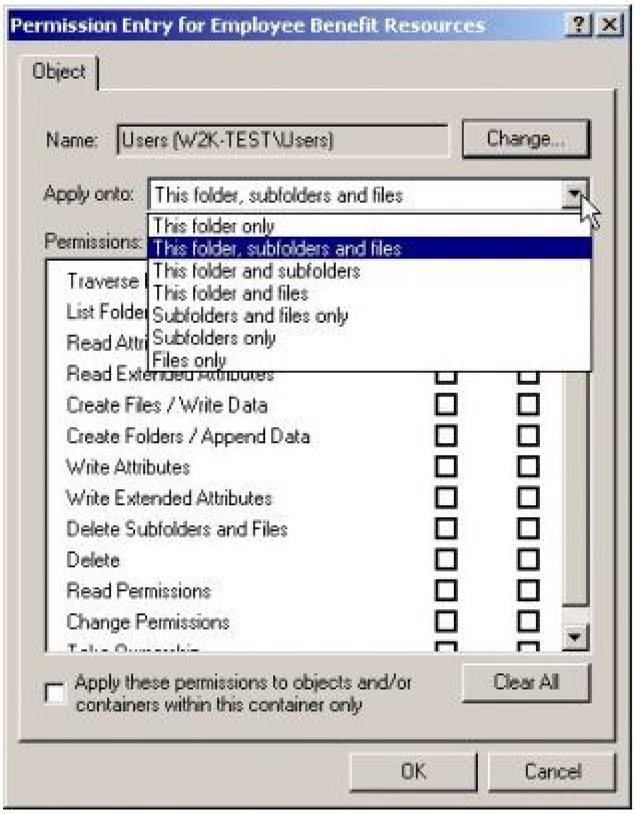
Synchronize	✓	✓	✓	✓	✓	✓

Although **List Folder Contents** and **Read & Execute** appear to have the same special permissions, these permissions are inherited differently. **List Folder Contents** is inherited by folders but not files, and it should only appear when viewing folder permissions. **Read & Execute** is inherited by both files and folders and is always present when viewing file or folder permissions.

Top Of Page

Selecting where to apply permissions

The **Permission Entry** dialog box appears when permissions are set on files and folders. In this dialog box, **Apply onto** lists the locations where permissions can be applied. How these permissions are applied depends on whether the **Apply these permissions to objects and/or containers within this container only** check box is selected. By default, this check box is clear.



Permission Entry for Employee Benefit Resources

Object

Name: Users (W2K-TEST\Users)

Apply onto: This folder, subfolders and files

- This folder only
- This folder, subfolders and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

Permissions:

Traverse		
List Folde		
Read Attri		
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	□	□

□ Apply these permissions to objects and/or containers within this container only

When the **Apply these permissions...** check box is clear, permissions are applied as shown below:

Apply onto	**Applies permissions to current folder**	**Applies permissions to subfolders in current folder**	**Applies permissions to files in current folder**	**Applies permissions to all subsequent subfolders**	**Applies permissions to files in all subsequent subfolders**
This folder only	✓				
The folder, subfolders and files	✓	✓	✓	✓	✓
This folder and subfolders	✓	✓		✓	

This folder and files	✓		✓		✓
Subfolders and files only		✓	✓	✓	✓
Subfolders only		✓		✓	
Files only			✓		✓

When the **Apply these permissions...** check box is selected, permissions are applied as shown below:

Apply onto	**Applies permissions to current folder**	**Applies permissions to subfolders in current folder**	**Applies permissions to files in current folder**	**Applies permissions to all subsequent subfolders**	**Applies permissions to files in all subsequent subfolders**
This folder only	✓				
The folder, subfolders and files	✓	✓	✓		
This folder and subfolders	✓	✓			
This folder and files	✓		✓		
Subfolders and files only		✓	✓		
Subfolders only		✓			
Files only			✓		

Top Of Page

Setting or modifying permissions

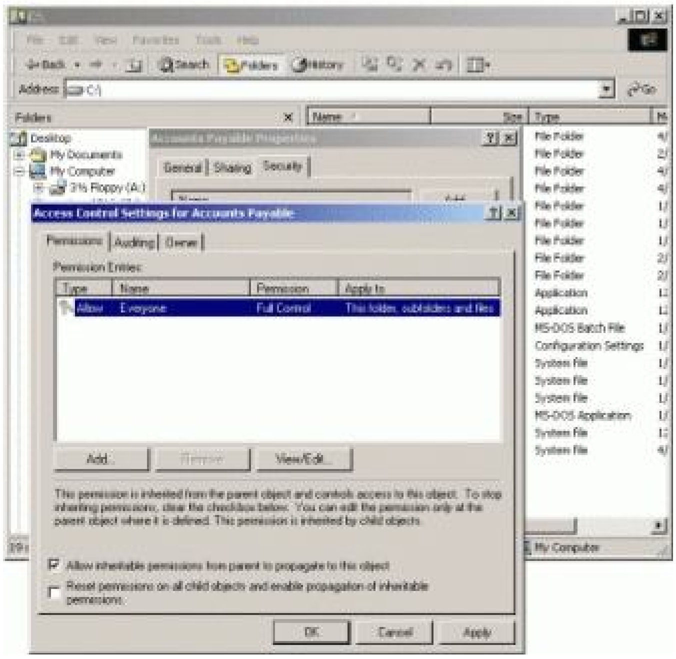
To set, view, change, or remove special permissions for files and folders:

1. Open Windows Explorer; click **Start**, point to **Programs**, point to **Accessories**, and then click **Windows Explorer**.

2. Locate the file or folder for which special permissions are to be set.

3. Right-click the file or folder, click **Properties**, and then click the **Security** tab.

4. Click **Advanced**.


File Edit View Favorites Tools Help
Back Search Folders History
Address C:\
Folders
Desktop
My Documents
My Computer
3½ Floppy (A:)
Accounts Payable Properties
General Sharing Security
Access Control Settings for Accounts Payable
Permissions Auditing Owner
Add... Remove View/Edit...
OK Cancel Apply
My Computer

Permission Entries:

Type	Name	Permission	Apply to
Allow	Everyone	Full Control	This folder, subfolders and files

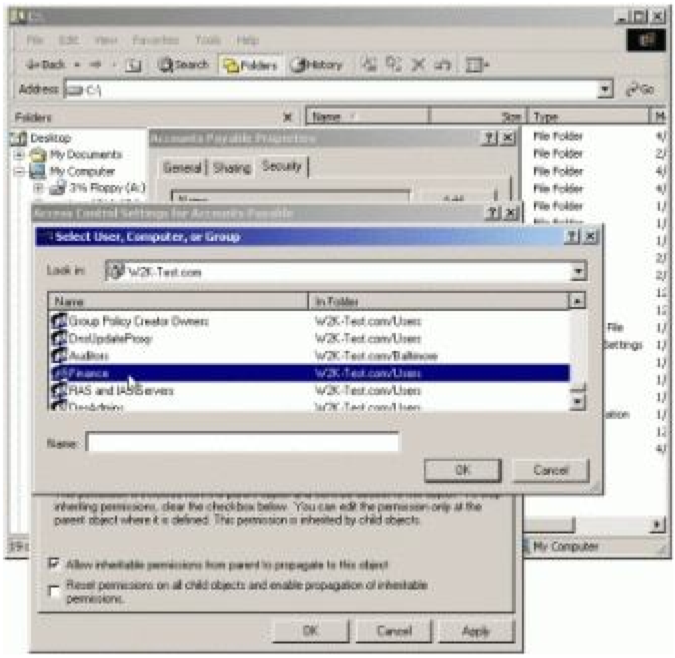
This permission is inherited from the parent object and controls access to this object. To stop inheriting permissions, clear the checkbox below. You can edit the permission only at the parent object where it is defined. This permission is inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

□ Reset permissions on all child objects and enable propagation of inheritable permissions.

5. Perform one of the following:

   - To set special permissions for a new group or user, click **Add**. In **Name**, type the name of the user or group using the format *domainname\name* or select from the list. To access account names from the domain, click the **Look In** list box. There should now be a list that shows the current machine, the local domain, trusted domains, and other resources that can be accessed. Select the local domain to view all the account names in the domain.


Select User, Computer, or Group
Access Control Settings for Accounts Payable
Accounts Payable Properties
General Sharing Security
OK Cancel
OK Cancel Apply
My Computer

Look in: W2K-Test.com

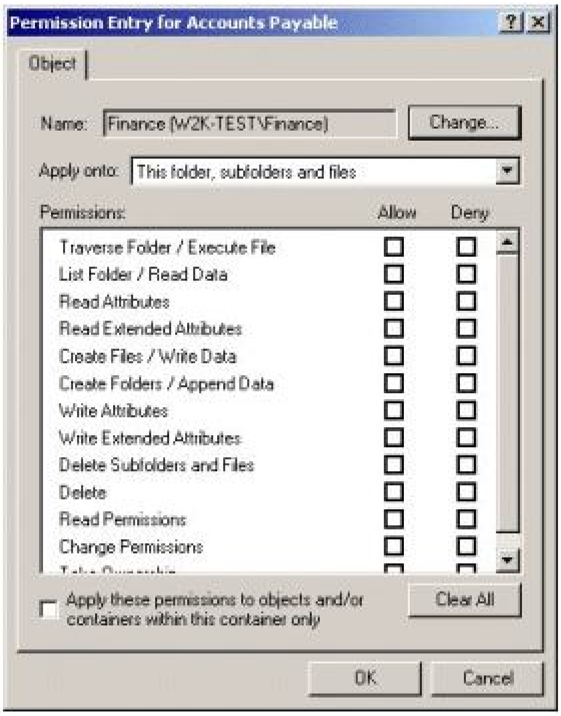
Name	In Folder
Group Policy Creator Owners	W2K-Test.com/Users
DnsUpdateProxy	W2K-Test.com/Users
Auditors	W2K-Test.com/Baltimore
Finance	W2K-Test.com/Users
RAS and IAS Servers	W2K-Test.com/Users
DnsAdmins	W2K-Test.com/Users

Name:

☑ Allow inheritable permissions from parent to propagate to this object

□ Reset permissions on all child objects and enable propagation of inheritable permissions.

   - When finished, click **OK** to automatically open the **Permission Entry** dialog box.



Permission Entry for Accounts Payable

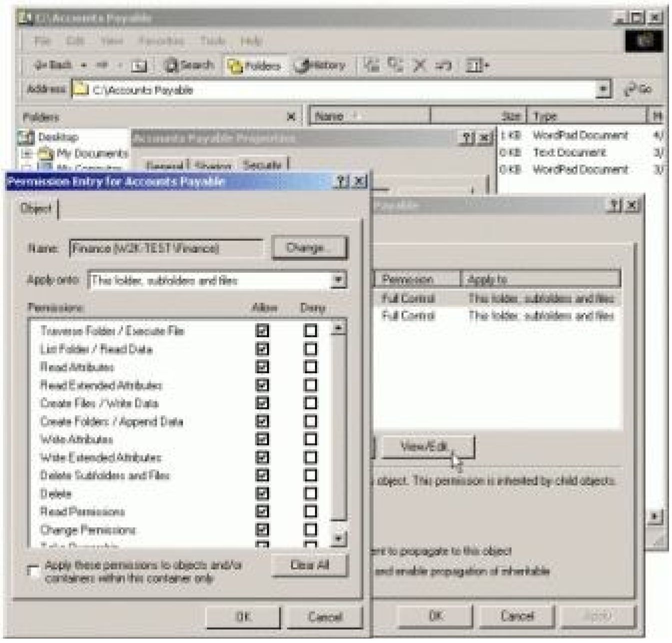
Name: Finance (W2K-TEST\Finance)

Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
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	□	□

□ Apply these permissions to objects and/or containers within this container only

- To view or change special permissions for an existing group or user, click the name of the group or user and then click **View/Edit**.



Permission Entry for Accounts Payable

Name: Finance (W2K-TEST\Finance)

Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
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	☑	□

□ Apply these permissions to objects and/or containers within this container only

Permission	Apply to
Full Control	This folder, subfolders and files
Full Control	This folder, subfolders and files

- To remove a group or user and its special permissions, click the name of the group or user and then click **Remove**. If the **Remove** button is unavailable, clear the **Allow inheritable permissions...** check box. The file or folder will no longer inherit permissions. Skip steps 4, 5, and 6.

6. In the **Permission Entry** dialog box, click where the permissions are to be applied in **Apply onto**, if necessary. **Apply onto** is available only for folders.

7. In **Permissions**, click **Allow** or **Deny** for each permission.

8. To prevent subfolders and files within the tree from inheriting these permissions, click to select the **Apply these permissions...** check box.

Note:

Permissions can only be set on drives formatted to use NTFS.

To change permissions, a user must be the owner or have been granted permission to do so by the owner.

If the check boxes under Permissions are shaded, the file or folder has inherited the permissions from the parent folder.**Warning:** Groups or users granted Full Control for a folder can delete files and subfolders within that folder regardless of the permissions protecting the files and subfolders.

Top Of Page

How inheritance affects file and folder permissions

After setting permissions on a parent folder, new files and subfolders created in the folder inherit these permissions. If inherited permissions are not desired, select **This folder only** in **Apply onto** when special permissions are set for the parent folder.

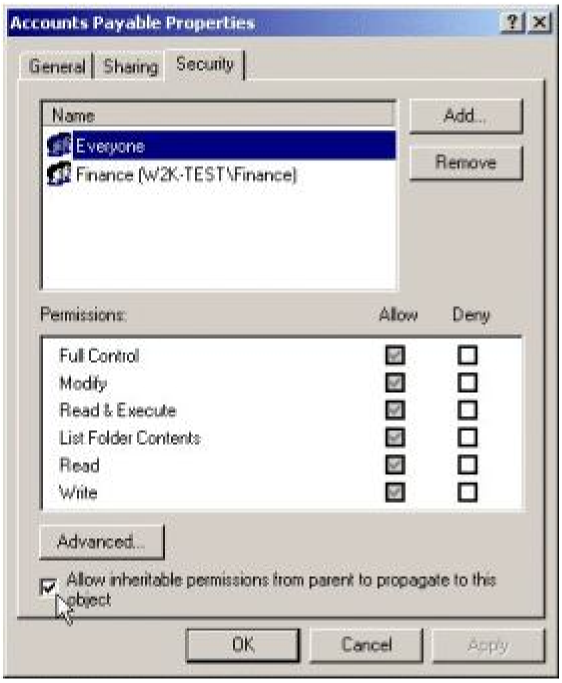
To prevent only certain files or subfolders from inheriting permissions:

1. Right-click the file or subfolder, click **Properties**, click the **Security** tab.

   If the permission check boxes for an account appear shaded, the file or folder has inherited permissions from the parent folder. There are three ways to make changes to inherited permissions:

   - Make the changes to the parent folder, and then the file or folder will inherit these permissions.
   - Select the opposite permission (**Allow** or **Deny**) to override the inherited permission.
   - Clear the **Allow inheritable permissions from parent to propagate to this object** check box. This will allow changes to the permissions or removal of the user or group from the permissions list. However, the file or folder will no longer inherit permissions from the parent folder.

2. Clear the **Allow inheritable permissions from parent to propagate to this object** check box.

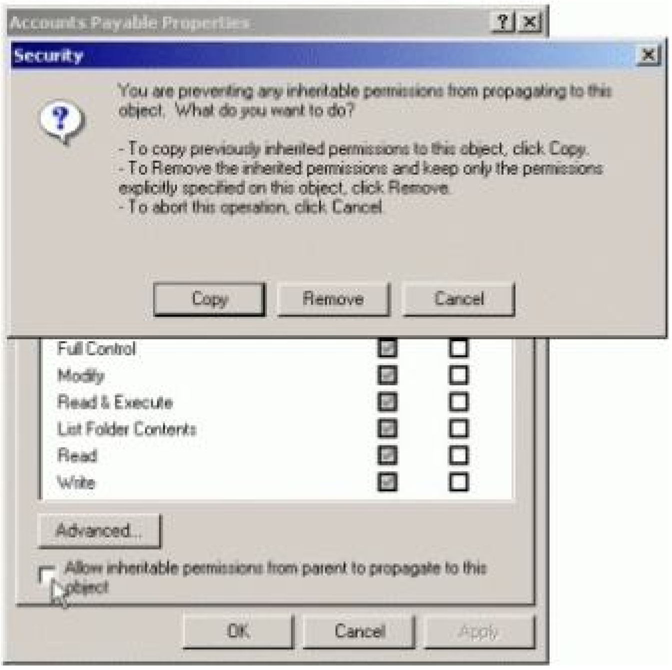


Name
Everyone
Finance (W2K-TEST\Finance)

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

3. A **Security** window, shown below, will appear asking whether to copy inherited permissions or remove them. Click on the **Remove** button.



Security

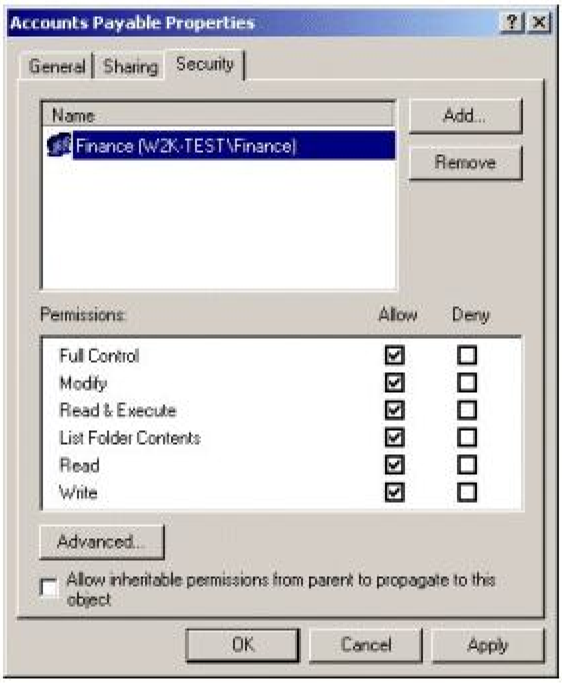
You are preventing any inheritable permissions from propagating to this object. What do you want to do?

- To copy previously inherited permissions to this object, click Copy.
- To Remove the inherited permissions and keep only the permissions explicitly specified on this object, click Remove.
- To abort this operation, click Cancel.

Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

4. All permissions previously inherited are removed from the file or subfolder.



Accounts Payable Properties

Name: Finance (W2K-TEST\Finance)

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

□ Allow inheritable permissions from parent to propagate to this object

If neither **Allow** nor **Deny** is selected for a permission, then the group or user may have obtained the permission through group membership. If the group or user has not obtained the permission through membership in another group, then the group or user is implicitly denied the permission. To explicitly allow or deny the permission, click the appropriate check box.

Top Of Page

Shared folder permissions

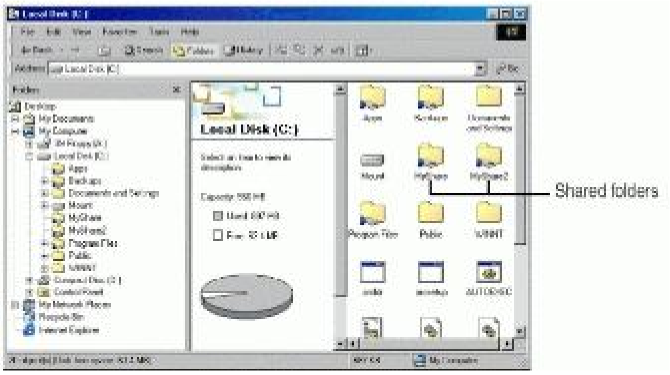
Shared folders are used to provide network users with access to files and application resources on the network. When a folder is shared, users can connect to the folder over the network and gain access to the files that it contains. However, to gain access to the files, users must have permissions to access the shared folders.

A shared folder can contain applications, data, or a user's personal data, called a home folder. Each type of data requires different shared folder permissions. The following are characteristics of shared folder permissions:

- Shared folder permissions apply to folders, not individual files. Since shared folder permissions can be applied only to the entire shared folder, and not to individual files or subfolders in the shared folder, shared folder permissions provide less detailed security than NTFS permissions.

- Shared folder permissions do not restrict access to users who gain access to the folder at the computer where the folder is stored. They apply only to users who connect to the folder over the network.
- Shared folder permissions are the only way to secure network resources on a File Allocation Table (FAT) volume. NTFS permissions are not available on FAT volumes.
- The default shared folder permission is Full Control, and it is assigned to the "Everyone" group when sharing the folder.

A shared folder appears in Windows Explorer as an icon of a hand holding the shared folder as shown below.



To control how users gain access to a shared folder, assign shared folder permissions. The following table shows shared folder permissions and the actions on shared folders allowed to users by the share permission.

Shared Folder Permission

Actions Allowed by Share Permissions	**Full Control**	**Change**	**Read**
Viewing file names and subfolder names	✓	✓	✓
Traversing to subfolders	✓	✓	✓
Viewing data in files and running programs	✓	✓	✓
Adding files and subfolders to the shared folder	✓	✓	
Changing data in files	✓	✓	
Deleting subfolders and files	✓	✓	
Changing permissions (NTFS only)	✓		
Taking ownership (NTFS only)	✓		

Shared folder permissions can be set to allow or deny. Generally, it is best to allow permissions and to assign those permissions to a group rather than to individual users. Deny permissions should only be used when it is necessary to override permissions that are otherwise applied. In most cases, deny permissions should only be applied when it is necessary to deny permission to a specific user who belongs to a group to which has been given the permission. If a shared folder is set with deny permission to a user, the user will not have that permission. For example, to deny all access to a shared folder, deny the Full Control permission.

How Shared Folder Permissions Are Applied

Applying shared permissions to user accounts and groups affects access to a shared folder. Denying permission takes precedence over the permissions that are allowed. The following list describes the effects of applying permissions.

- **Multiple Permissions Combine:** A user can be a member of multiple groups, each with different permissions that provide different levels of access to a shared folder. When permission is assigned to a user for a shared folder, and that user is a member of a group that is assigned a different permission, the user's effective permissions are the combination of the user and group permissions. For example, if a user has Read permission and is a member of a group with Change permission, the user's effective permission is Change, which includes Read.

- **Denying Permissions Overrides Other Permissions:** Denied permissions take precedence over any permissions that are otherwise allowed for user accounts and groups. If a user is denied permission to a shared folder, the user will not have that permission, even if allowed the permission for a group of which the user is a member.

- **NTFS Permissions Are Required on NTFS Volumes:** Shared folder permissions are sufficient to gain access to files and folders on a FAT volume but not on an NTFS volume. On a FAT volume, users can gain access to a shared folder for which they have permissions, as well as all of the folder's contents. When users gain access to a shared folder on an NTFS volume, they need the shared folder permission and also the appropriate NTFS permissions for each file and folder to which they gain access.

- **Copied or Moved Shared Folders Are No Longer Shared:** When a shared folder is copied, the original shared folder is still shared, but the copy is not shared. When a shared folder is moved, it is no longer shared.

Guidelines for Shared Folder Permissions

The following list provides some general guidelines for managing shared folders and assigning shared folder permissions:

- Determine which groups need access to each resource and the level of access that they require. Document the groups and their permissions for each resource.

- Assign permissions to groups instead of user accounts to simplify access administration.

- Assign to a resource the most restrictive permissions that still allow users to perform required tasks. For example, if users need only to read information in a folder, and they will never delete or create files, assign the Read permission.

- Organize resources so that folders with the same security requirements are located within a common parent folder. For example, if users require Read permission for several application folders, store the application folders within the same parent folder. Then share this folder instead of sharing each individual application folder.

- Use intuitive share names so that users can easily recognize and locate resources. For example, for the Application folder, use Apps for the share name. Also use share names that all client operating systems can use.

Microsoft Windows 2000 provides 8.3-character equivalent names, but the resulting names might not be intuitive to users. For example, a Windows 2000 folder named Accountants Database would appear as Account~1 on client computers running MS-DOS, Windows 3.x, and Windows for Workgroups.

Sharing Folders

Share resources with others by sharing the folders containing those resources. To share a folder, a user must be a member of one of several groups, depending on the role of the computer where the shared folder resides. When a folder is shared, access to the folder can be controlled by placing a limit on the number of users who can simultaneously access it, and access to the folder and its contents can also be controlled by assigning permissions to selected users and groups. Which groups can share folders and on which machines they can share them depends on whether it is a workgroup or a domain and the type of computer on which the shared folders reside:

- In a Windows 2000 domain, the Administrators and Server Operators groups can share folders residing on any machines in the domain. The Power Users group is a local group and can share folders residing only on the stand-alone server or computer running Windows 2000 Professional where the group is located.

- In a Windows 2000 workgroup, the Administrators and Power Users groups can share folders on the Windows 2000 Server stand-alone server or the computer running Windows 2000 Professional on which the group exists.

If the folder to be shared resides on an NTFS volume, users must also have at least the Read permission for that folder to be able to share it.

Administrative Shared Folders

Windows 2000 automatically shares folders for administrative purposes. These shares are appended with a dollar sign ($), which hides the shared folder from users who browse the computer through the network. The root of each volume, the system root folder, and the location of the printer drivers are all hidden shared folders. The following table describes the purpose of the administrative shared folders that Windows 2000 automatically provides. These shares can be disabled, but only for the current session. When Windows 2000 is restarted, the shares will be re-enabled. The permissions on these shares cannot be changed.

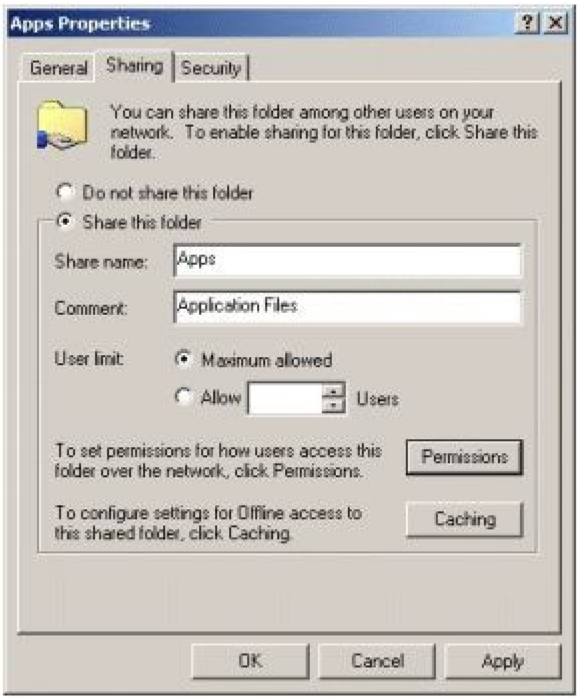
Share	**Purpose**
C$, D$, E$, and so on	The root of each volume on a hard disk is automatically shared, and the share name is the drive letter appended with a dollar sign ($). Connecting to this folder, allows access to the entire volume. Use the administrative shares to remotely connect to the computer to perform administrative tasks. Windows 2000 assigns the Full Control permission to the Administrators group. Windows 2000 also automatically shares CD-ROM drives and creates the share name by appending the dollar sign to the CD-ROM drive letter.
ADMIN$	The system root folder, which is C:\Winnt by default, is shared as Admin$. Administrators can gain access to this shared folder to administer Windows 2000 without knowing in which folder it is installed. Only members of the Administrators group have access to this share. Windows 2000 assigns the Full Control permission to the Administrators group.
IPC$	Interprocess communication share.
Print$	When the first shared printer is installed, the systemroot\ System32\Spool\Drivers folder is shared as Print$. This folder provides access to printer driver files for clients. Only members of the Administrators, Server Operators, and Print Operators groups have the Full Control permission. The Everyone group has the Read permission.

Hidden shared folders are not limited to those that the system automatically creates. Additional folders can be shared and a dollar sign can be appended to the end of the share name. Then only users who know the folder name can gain access to it if they also possess the proper permissions to it.

Sharing a Folder

When a folder is shared, it can be given a share name, comments can be provided to describe the folder and its content, limits to the number of users who have access to the folder can be set, permissions can be assigned, and the folder can be shared multiple times. A folder can be shared as follows:

1. Log on with a user account that is a member of a group that is able to share folders.
2. Right-click the folder that is to be shared, and then click **Sharing . . .** . The folder's properties window will appear, showing the options of the **Sharing** tab.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Apps

Comment: Application Files

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

3. On the **Sharing** tab of the **Properties** dialog box, configure the options shown in the table below to make the folder available as a share.

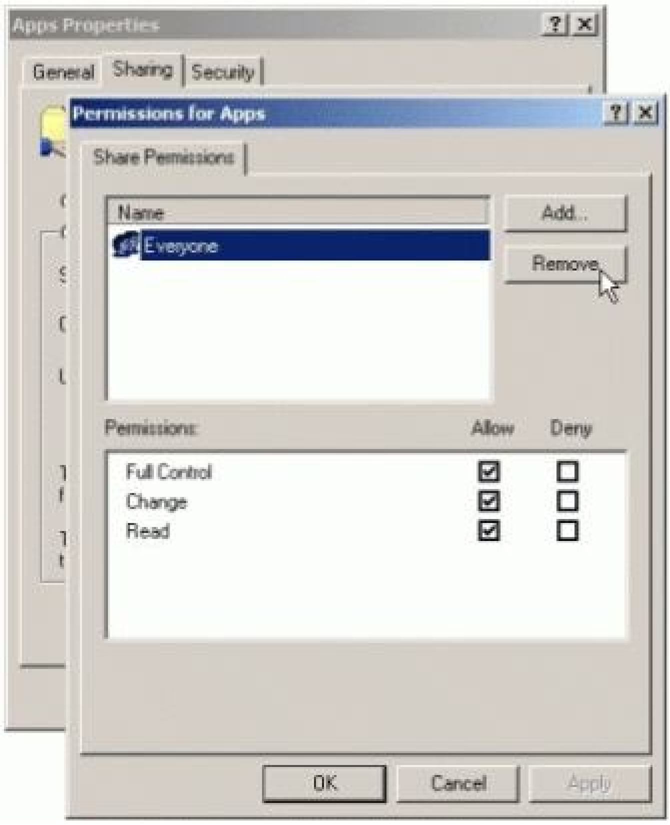
Option	**Description**
Share Name	The name that users from remote locations use to make a connection to the shared folder. A share name must be entered.
Comment	An optional description for the share name. The comment appears in addition to the share name when users at client computers browse the server for shared folders. This comment can be used to identify contents of the shared folder.
User Limit	The number of users who can concurrently connect to the shared folder. If **Maximum allowed** is selected as the user limit, Windows 2000 Professional supports up to 10 connections. Windows 2000 Server can support an unlimited number of connections, but the number of Client Access Licenses (CALs) that are purchased limits the connections.
Permissions	The shared folder permissions that apply only when the folder is accessed over the network. By default, the Everyone group is assigned Full Control for all new shared folders.
Caching	The settings to configure offline access to this shared folder.

Assigning Shared Folder Permissions

After sharing a folder, the next step is to specify which users have access to the shared folder by assigning shared folder permissions to selected user accounts and groups. Assign permissions to user accounts and groups for a shared folder, as follows:

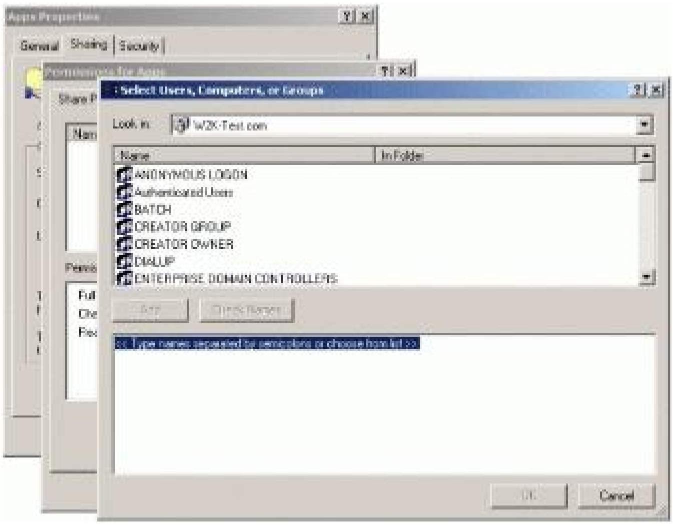
1. On the **Sharing** tab of the Properties dialog box of the shared folder, click **Permissions**.

2. In the **Permissions** dialog box, ensure that the Everyone group is selected and then click **Remove**.



Permissions:	Allow	Deny
Full Control	☑	☐
Change	☑	☐
Read	☑	☐

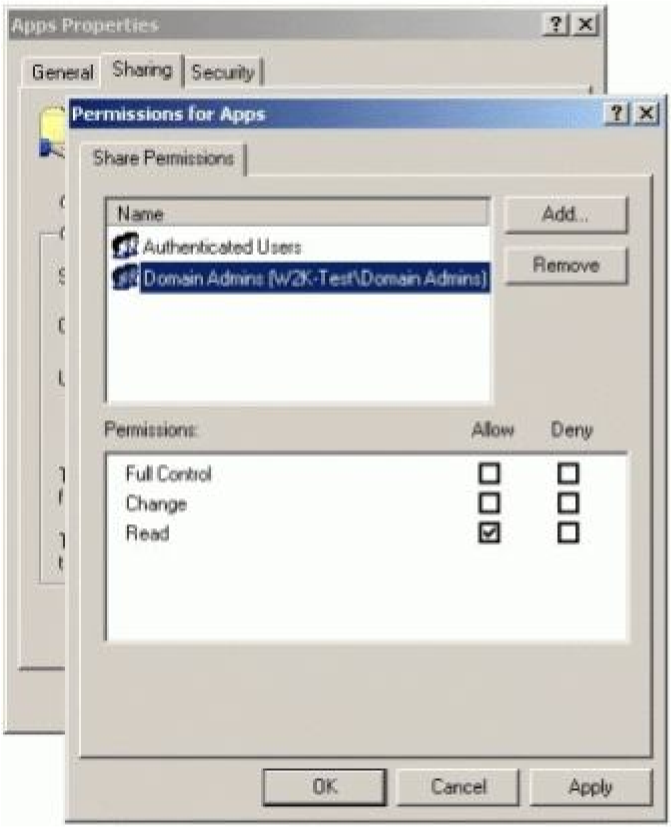
3. In the **Permissions** dialog box, click **Add**.



4. In the **Select Users, Computers, Or Groups** dialog box, click the user accounts and groups to which permissions are to be assigned.

5. Click **Add** to add the user account or group to the shared folder. Repeat this step for all user accounts and groups to which permissions are to be assigned.

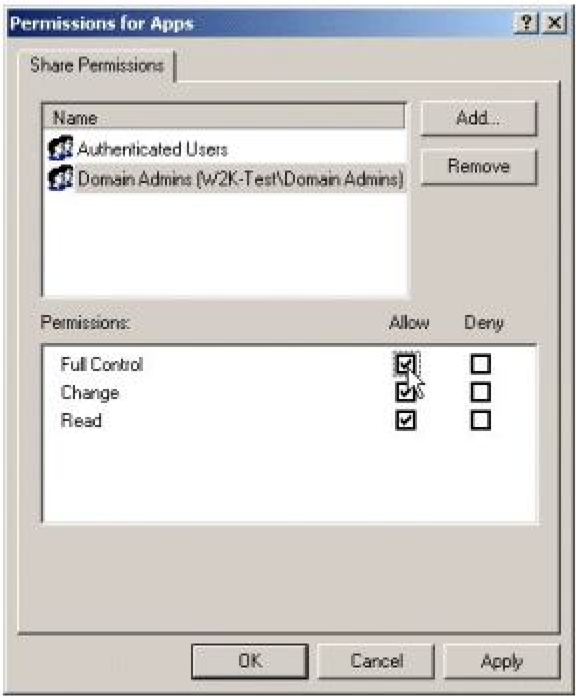
6. Click **OK**.



Name
Authenticated Users
Domain Admins (W2K-Test\Domain Admins)

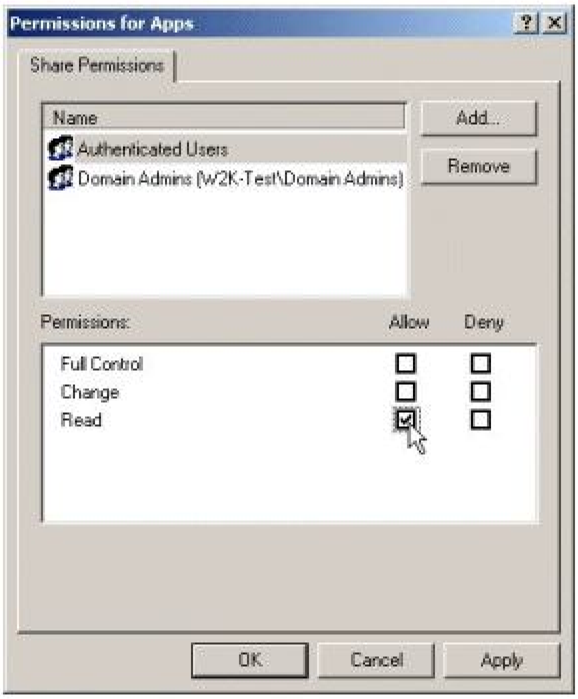
Permissions:	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

7. In the **Permissions** dialog box for the shared folder, click the user account or group, and then, under **Permissions**, select the **Allow** check box or the **Deny** check box for the appropriate permissions for the user account or group.



Name
Authenticated Users
Domain Admins (W2K-Test\Domain Admins)

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□



Permissions for Apps

Share Permissions

Name
Authenticated Users
Domain Admins (W2K-Test\Domain Admins)

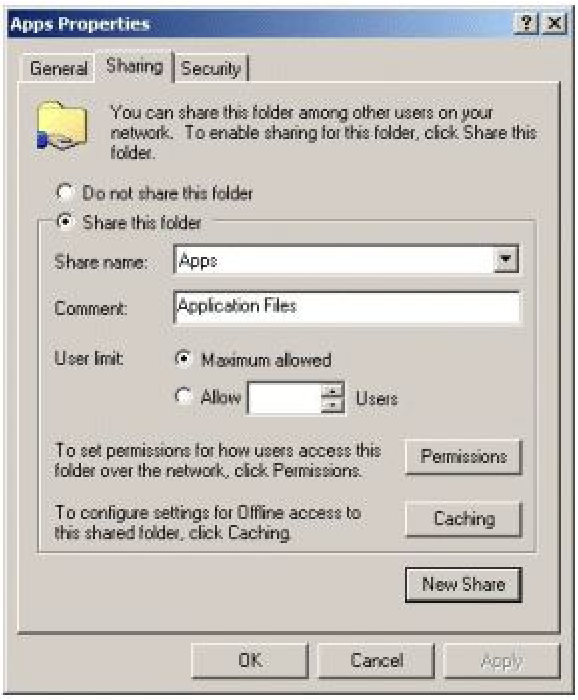
Permissions:	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Modifying Shared Folders

Authorized users can modify shared folders, stop sharing a folder, modify the share name, and modify shared folder permissions.

Authorized users can modify a shared folder as follows:

1. Click the **Sharing** tab in the **Properties** dialog box of the shared folder.



Apps Properties

General | Sharing | Security

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Apps

Comment: Application Files

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

2. To complete the appropriate task, use the steps in the table below.

To	Do this
Stop sharing a folder	Click **Do not share this folder**.

Modify the share name	Click **Do not share this folder** to stop sharing the folder; click **Apply** to apply the change; click **Share this folder**, and then enter the new share name in the **Share name** box.
Modify shared folder permissions	Click **Permissions**. In the **Permissions** dialog box, click **Add** or **Remove**. In the **Name** dialog box, click the user account or group whose permissions are to be modified. Modify the permissions in the **Permissions: Allow** or **Deny** dialog box.
Share folder multiple times	Click **New Share** to share a folder with an additional shared folder name. Do so to consolidate multiple shared folders into one while allowing users to continue to use the same shared folder name that they used before consolidating the folders.
Remove a share name	Click **Remove Share**. This option appears only after the folder has been shared more than once.

Note: If sharing is disabled on a folder while a user has a file open, the user might lose data. If **Do not share this folder** is selected while a user has a connection to the shared folder, Windows 2000 displays a notification that a user has a connection to the shared folder.

Combining Shared Folder Permissions and NTFS Permissions

Folders can be shared to provide network users with access to resources. If using a FAT volume, the shared folder permissions are the only resource available to provide security for the folders that are shared and the folders and files they contain. If using an NTFS volume, NTFS permissions can be assigned to individual users and groups to better control access to the files and subfolders in the shared folders. When combining shared folder permissions and NTFS permissions, the more restrictive permission is always the overriding permission.

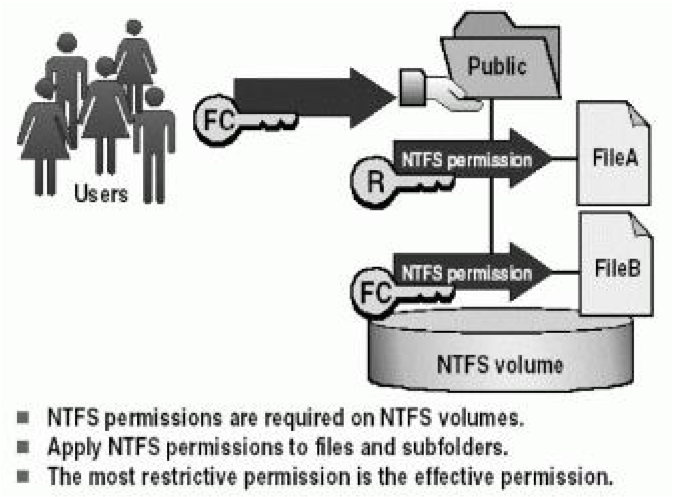
One strategy for providing access to resources on an NTFS volume is to share folders with the default shared folder permissions and then control access by assigning NTFS permissions. When a folder is shared on an NTFS volume both shared folder permissions and NTFS permissions combine to secure file resources.

Shared folder permissions provide limited security for resources. The greatest flexibility can be gained by using NTFS permissions to control access to shared folders. Also, NTFS permissions apply whether the resource is accessed locally or over the network.

When using shared folder permissions on an NTFS volume, the following rules apply:

- NTFS permissions can be applied to files and subfolders in the shared folder. Different NTFS permissions can be applied to each file and subfolder that a shared folder contains.
- In addition to shared folder permissions, users must have NTFS permissions for the files and subfolders that shared folders contain to gain access to those files and subfolders. This is in contrast to FAT volumes where permissions for a shared folder are the only permissions protecting files and subfolders in the shared folder.
- When combining shared folder permissions and NTFS permissions, the more restrictive permission is always the overriding permission.

In the figure below, the Everyone group has the shared folder Full Control permission for the Public folder and the NTFS Read permission for File A. The Everyone group's effective permission for File A is Read because Read is the more restrictive permission. The effective permission for File B is Full Control because both the shared folder permission and the NTFS permission allow this level of access.



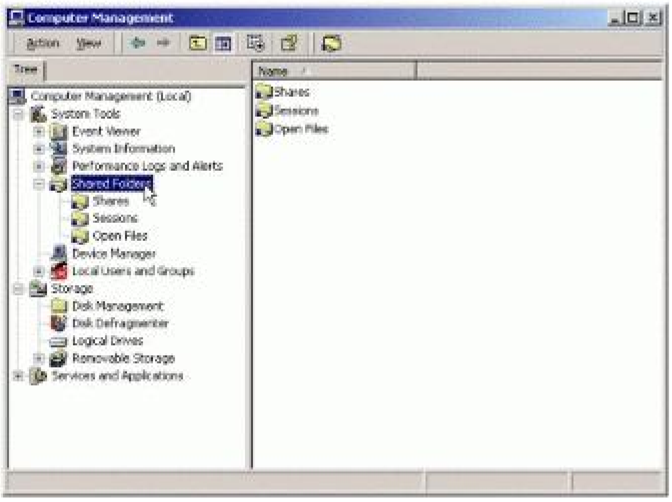
- NTFS permissions are required on NTFS volumes.
- Apply NTFS permissions to files and subfolders.
- The most restrictive permission is the effective permission.

Disconnecting a user or users from a share or active session

Authorized users can manage shares and disconnect active sessions from the Shared Folders object in the **Computer Management** GUI. For Windows 2000 Professional, only members of the Administrators or Power Users group can use Shared Folders. For Windows 2000 Server, members of the Server Operators group can also use Shared Folders. Note that disconnecting users who are using resources may result in loss of data. It is a good idea to warn connected users before disconnecting them.

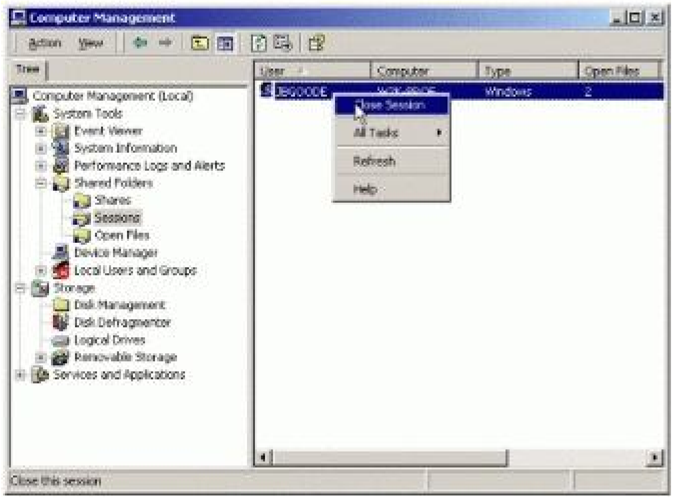
Disconnect a user or users as follows:

1. Click **Start**, select **Programs**, select **Administrative Tools**, click **Computer Management**, and then double-click **Shared Folders**.

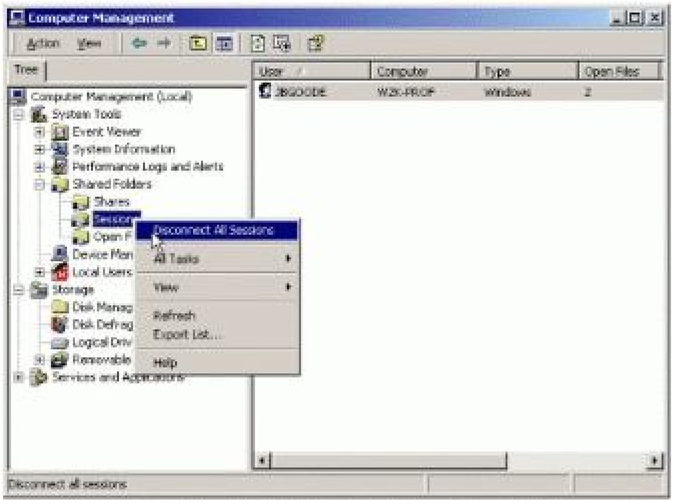


2. In the console tree, click **Sessions**.

3. To disconnect one user, right-click the user name and then click **Close Session**.



4. To disconnect all users, right-click **Sessions**, and then click **Disconnect All Sessions**.



Top Of Page

Active Directory object permissions

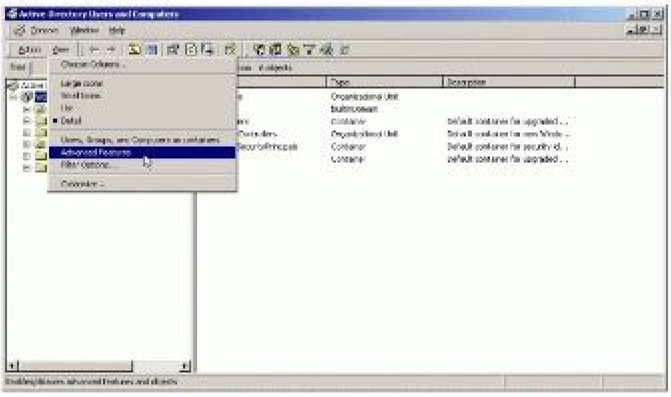
In controlling access to Active Directory objects, there are two things to consider: the permissions that a user is allowed to attach to the object and the ways in which these permissions can be attached in order to delegate administrative responsibility for Active Directory objects.

Active Directory objects can have the following permissions attached to them:

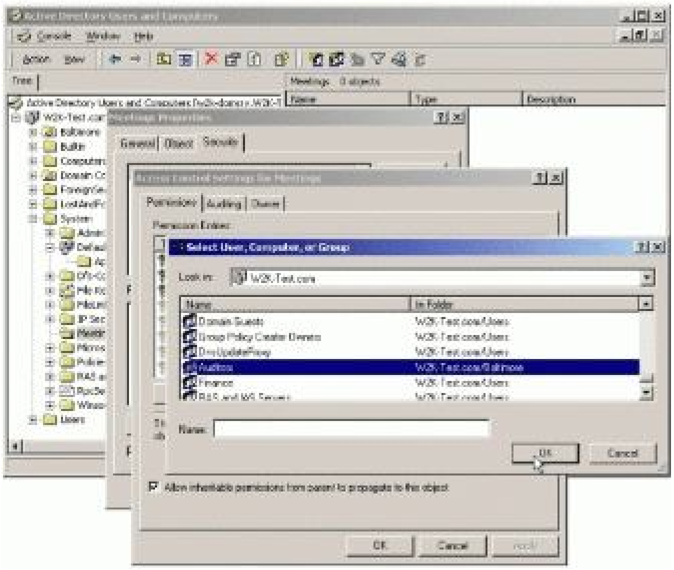
- Create Child (can be specific to the type of object or general for any object under the container)
- Delete Child (can be specific to the type of object or general for any object under the container)
- Read Property (can be specific to an individual property of the object or general for all attributes of the object)
- Write Property (can be specific to an individual property of the object or general for all attributes of the object)
- List Contents
- Write Self
- Delete Tree
- List Object
- Control Access (can be specific to an individual control operation or general for all control operations on the object)

Permissions can be set on a directory object using the following procedure:

1. Log on using an administrator account.
2. Open the **Active Directory Users and Computers** tool.
3. On the **View** menu, select **Advanced Features**.

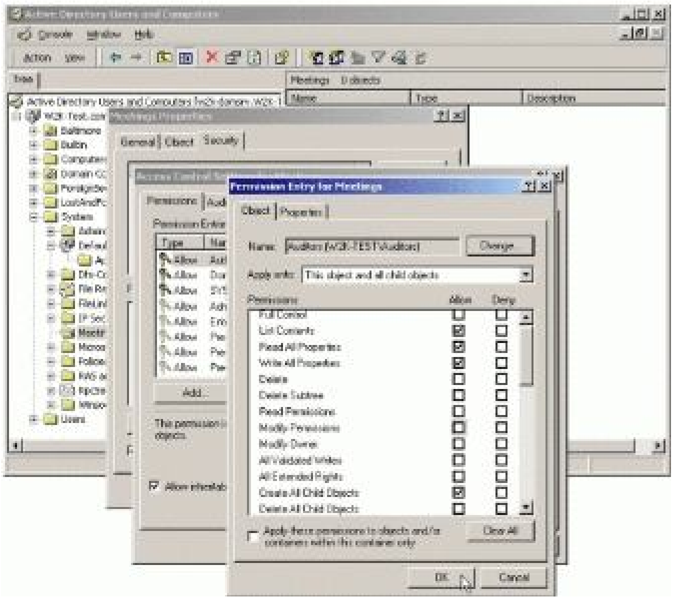


4. Locate the container for the object, right-click it, and then click **Properties**.
5. Click the **Security** tab, and click **Advanced**.
6. In the **Permissions** window, and click the **Add** button.
7. Select a security principle name and click **OK**.



Name	In Folder
Domain Guests	W2K-Test.com/Users
Group Policy Creator Owners	W2K-Test.com/Users
DnsUpdateProxy	W2K-Test.com/Users
Auditors	W2K-Test.com/Baltimore
Finance	W2K-Test.com/Users
RAS and IAS Servers	W2K-Test.com/Users

8. There will be a dialog box with two tabs—**Object** and **Properties**.
9. The **Object** tab allows an authorized administrator to specify access permissions to the object.
10. The **Properties** tab allows an authorized administrator to specify access permissions to the object properties.
11. Use the pull-down lists to make selections.
12. Click each tab that is to be modified, and select the check boxes for the permissions to be set.
13. Check the **Apply . . .** box and then click **OK**.



Permission Entry for Meetings

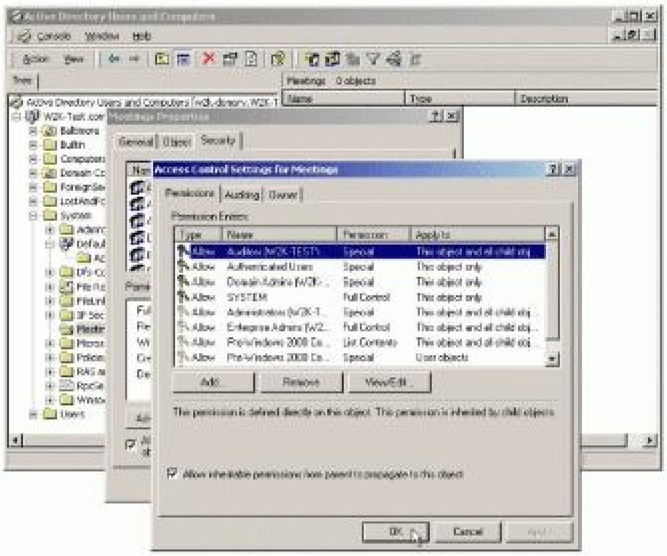
Name: Auditors (W2K-TEST\Auditors)

Apply onto: This object and all child objects

Permissions	Allow	Deny
Full Control	□	□
List Contents	☑	□
Read All Properties	☑	□
Write All Properties	☑	□
Delete	□	□
Delete Subtree	□	□
Read Permissions	□	□
Modify Permissions	□	□
Modify Owner	□	□
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	☑	□
Delete All Child Objects	□	□

□ Apply these permissions to objects and/or containers within this container only

14. In the **Access Control Settings** window, choose whether the choices will be inherited from the parent container to this object. If yes, then select the **Allow inheritable auditing entries from parent to propagate to this object** check box.



Access Control Settings for Meetings

Permission Entries:

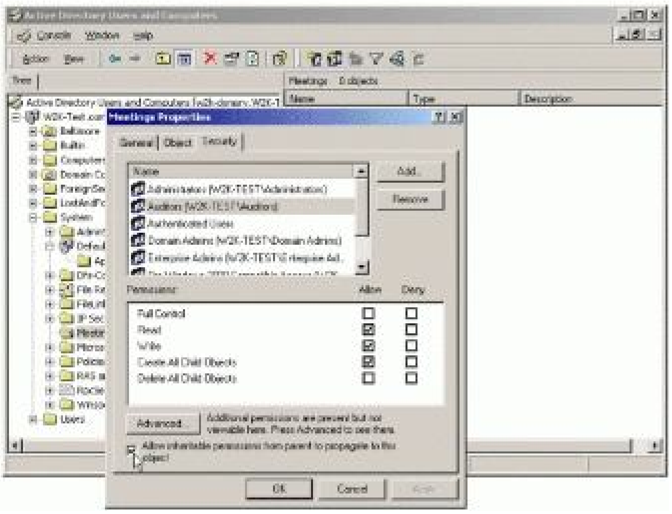
Type	Name	Permission	Apply to
Allow	Auditors (W2K-TEST\...	Special	This object and all child obj...
Allow	Authenticated Users	Special	This object only
Allow	Domain Admins (W2K-...	Special	This object only
Allow	SYSTEM	Full Control	This object only
Allow	Administrators (W2K-T...	Special	This object and all child obj...
Allow	Enterprise Admins (W2...	Full Control	This object and all child obj...
Allow	Pre-Windows 2000 Co...	List Contents	This object and all child obj...
Allow	Pre-Windows 2000 Co...	Special	User objects

This permission is defined directly on this object. This permission is inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

15. Click **Apply**, and then click **OK**.

16. In the Properties window, decide whether permissions must be inherited from the parent container to propagate this object. If yes, then check the appropriate box.



Meetings Properties

Name:
- Administrators (W2K-TEST\Administrators)
- Auditors (W2K-TEST\Auditors)
- Authenticated Users
- Domain Admins (W2K-TEST\Domain Admins)
- Enterprise Admins (W2K-TEST\Enterprise Ad...

Permissions:	Allow	Deny
Full Control	□	□
Read	☑	□
Write	☑	□
Create All Child Objects	☑	□
Delete All Child Objects	□	□

Additional permissions are present but not viewable here. Press Advanced to see them.

☑ Allow inheritable permissions from parent to propagate to this object

17. Click **Apply** and then click **OK**.

Top Of Page

Setting printer security permissions and shares

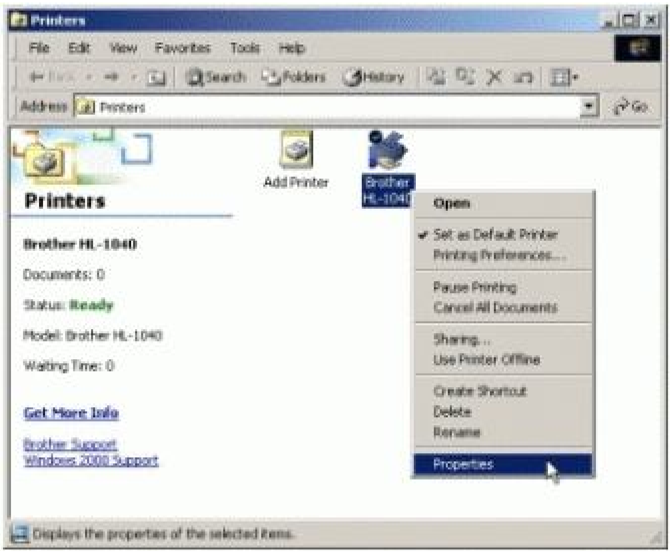
When a printer is installed on a network, default permissions are assigned that allow all users to print, and allow select groups to manage the printer, the documents sent to it, or both. Because the printer is available to all users on the network, it might be necessary to limit access for some users by assigning specific printer permissions. For example, all non-administrative users in a department could be given the Print permission and all managers could be given the Print and Manage Documents permissions. In this way, all users and managers can print documents, but managers can also change the print status of any document sent to the printer.

Windows 2000 provides three levels of printing security permissions: **Print**, **Manage Printers**, and **Manage Documents**. When multiple permissions are assigned to a group of users, the least restrictive permissions apply. However, when **Deny** is applied, it takes precedence over any permission. The table below provides a brief explanation of the types of tasks a user can perform at each permission level.

Permission	**Description**
Print	The user can connect to a printer and send documents to the printer. By default, the Print permission is assigned to all members of the Everyone group.
Manage Printers	The user can perform the tasks associated with the Print permission and has complete administrative control of the printer. The user can pause and restart the printer, change spooler settings, share a printer, adjust printer permissions, and change printer properties. By default, the Manage Printers permission is assigned to members of the Administrators and Power Users groups. By default, members of the Administrators and Power Users groups have full access, which means that the users are assigned the Print, Manage Documents, and Manage Printers permissions.
Manage Documents	The user can pause, resume, restart, and cancel documents submitted by all other users. The user cannot, however, send documents to the printer or control the status of the printer. By default, the Manage Documents permission is assigned to members of the Creator Owner group. When a user is assigned the Manage Documents permission, the user cannot access existing documents currently waiting to print. The permission will only apply to documents sent to the printer after the permission is assigned to the user.
Deny	Any or all of the preceding permissions are denied for the printer. When access is denied, the user cannot use or manage the printer, manipulate documents sent to the printer, or adjust any of the permissions.

Use the following procedures to set or remove permissions for a printer:

1. Click **Start**, point to **Settings**, and then click **Printers**.
2. Right-click the printer object for which permissions are to be set, click **Properties**.



Printers

Brother HL-1040

Documents: 0

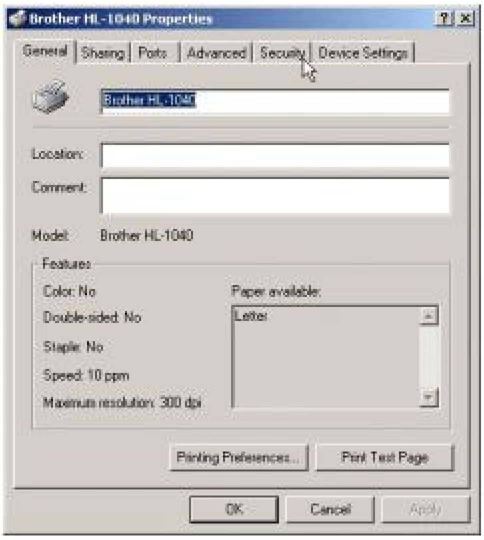
Status: Ready

Model: Brother HL-1040

Waiting Time: 0

Displays the properties of the selected items.

3. The printer **Properties** dialog window will appear.



Brother HL-1040

Location:

Comment:

Model: Brother HL-1040

Features

Color: No

Double-sided: No

Staple: No

Speed: 10 ppm

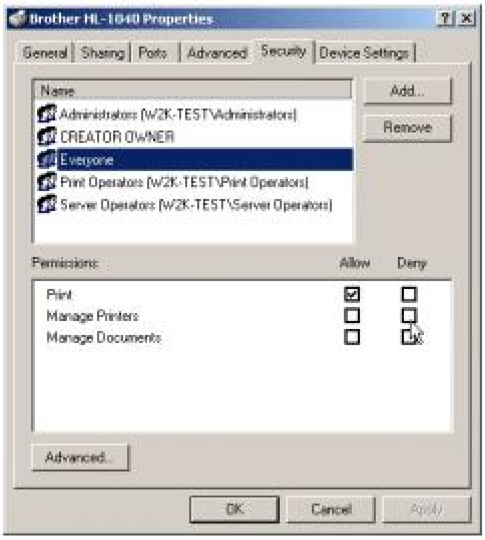
Maximum resolution: 300 dpi

Paper available:

Letter

4. Click the **Security** tab and do one of the following:

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



Name

Administrators (W2K-TEST\Administrators)

CREATOR OWNER

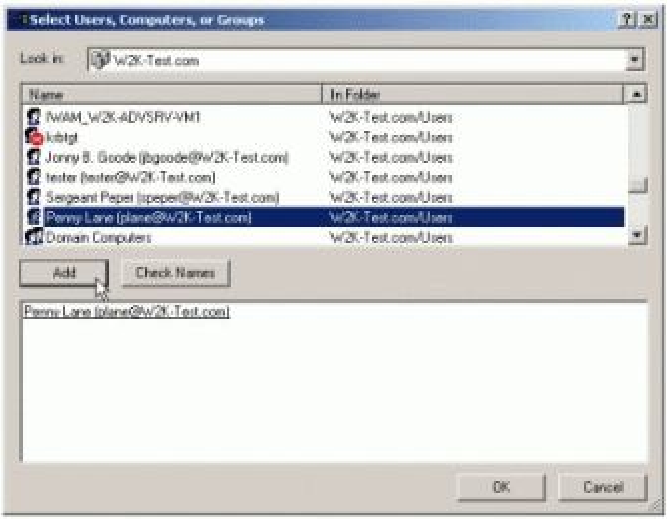
Everyone

Print Operators (W2K-TEST\Print Operators)

Server Operators (W2K-TEST\Server Operators)

Permissions:	Allow	Deny
Print	☑	□
Manage Printers	□	□
Manage Documents	□	□

- To set up permissions for a new user or group, click **Add**. In **Name**, type the name of the user or group to set permissions for, click **Add**, and then click **OK** to close the dialog box.



Look in: W2K-Test.com

Name	In Folder
IWAM_W2K-ADVSRV-VM1	W2K-Test.com/Users
krbtgt	W2K-Test.com/Users
Jonny B. Goode (jbgoode@W2K-Test.com)	W2K-Test.com/Users
tester (tester@W2K-Test.com)	W2K-Test.com/Users
Sergeant Peper (speper@W2K-Test.com)	W2K-Test.com/Users
Penny Lane (plane@W2K-Test.com)	W2K-Test.com/Users
Domain Computers	W2K-Test.com/Users

Penny Lane (plane@W2K-Test.com)

- In **Permissions**, click **Allow** or **Deny** for each permission that is to be allowed or denied for a selected user or group. Or, to remove the user or group from the permissions list, select the user or group and click **Remove**.

- After making all necessary permission assignments, click the **Apply** and then click **OK** on the printer **Properties** window.

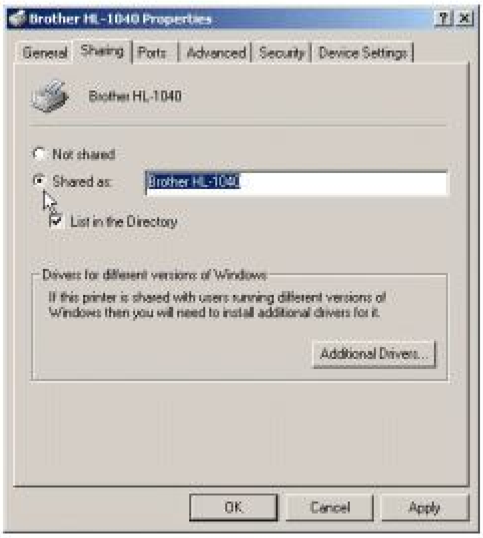
  Note: To change device settings, a user must have the **Manage Printers** permission. To view or change the underlying permissions that make up Print, Manage Printers, and Manage Documents, click the **Advanced** button.

  Printers are not shared by default when they are installed on Windows 2000 Professional. On Windows 2000 Server, the printer is shared by default when a printer is added. Use the following procedures to share a printer (a printer must be shared in order for the permission settings to affect the users and groups listed):

5. Click **Start**, point to **Settings**, and then click **Printers**.

6. Right-click the printer to be shared, and click the **Sharing** tab.

7. On the **Sharing** tab, click **Shared as** and then type a name for the shared printer.



Brother HL-1040

○ Not shared

● Shared as: Brother HL-1040

☑ List in the Directory

Drivers for different versions of Windows

If this printer is shared with users running different versions of Windows then you will need to install additional drivers for it.

8. If the printer is to be shared with users on different hardware or different operating systems, click **Additional Drivers**. Click the environment and operating system for the other computers, and then click **OK** to install the additional drivers.

9. If logged on to a Windows 2000 domain, the printer can be made available to other users on the domain by checking **List in the Directory** to publish the printer in the Directory.

10. Click **OK**.

Delegating administrative control

An authorized administrator can define delegation of responsibility to create new users or groups at the level of the organizational unit, or container, where the accounts are created. Group administrators for one organizational unit do not necessarily have the ability to create and manage accounts for another organizational unit within a domain. However, policy settings that are domain wide and permissions that are defined at higher levels in the directory tree can apply throughout the tree by using inheritance of permissions.

There are three ways to define the delegation of administration responsibilities:

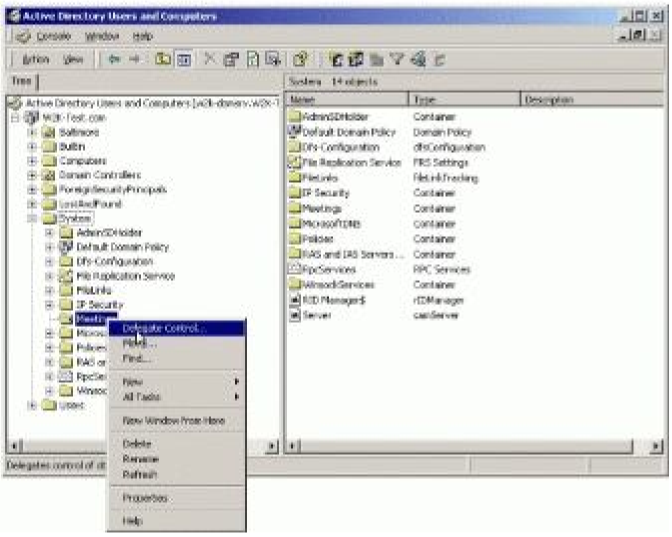
- Delegate permissions to change properties on a particular container.
- Delegate permissions to create and delete objects of a specific type under an organizational unit, such as users, groups, or printers.
- Delegate permissions to update specific properties on objects of a specific type under an organizational unit. For example, the right to set a password on a User object can be delegated.

An authorized administrator can delegate administration of particular resources to a specific individual or group, eliminating the need for multiple administrators to have authority over an entire domain or site. With appropriate delegation, the user or group who has been granted the appropriate permissions can, in turn, delegate administration of a subset of their accounts and resources.

The administrator can configure the scope of delegated administrative responsibility in many different ways. Although authorized administrators can generally grant permissions at the organizational unit level by applying inheritance, they can also delegate administration for an entire domain within a forest.

An authorized administrator can delegate administration of a domain or organizational unit by using the **Delegation of Control Wizard** available in **Active Directory Users and Computers**:

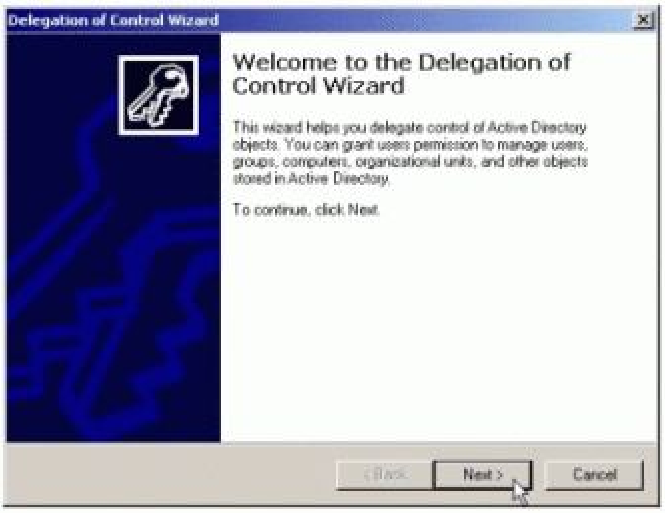
1. Log on using an administrator account.
2. Open the **Active Directory Users and Computers** tool.
3. Locate the container for the object, right-click it, and then click **Delegate Control. . .**.



System   14 objects

Name	Type	Description
AdminSDHolder	Container	
Default Domain Policy	Domain Policy	
Dfs-Configuration	dfsConfiguration	
File Replication Service	FRS Settings	
FileLinks	FileLinkTracking	
IP Security	Container	
Meetings	Container	
MicrosoftDNS	Container	
Policies	Container	
RAS and IAS Servers ...	Container	
RpcServices	RPC Services	
WinsockServices	Container	
RID Manager$	rIDManager	
Server	samServer	

4. The Delegation of **Control Wizard** appears, click **Next**.

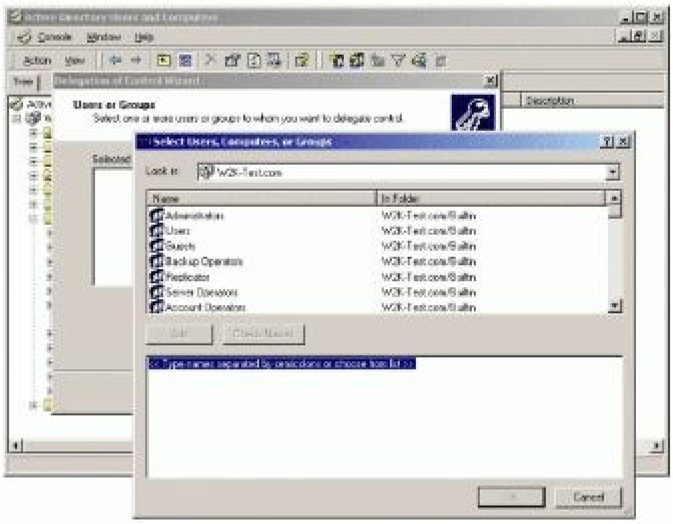


Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory.

To continue, click Next.

5. A Wizard window appears for selection of **Users or Groups**, click the **Add** button.



Users or Groups
Select one or more users or groups to whom you want to delegate control.

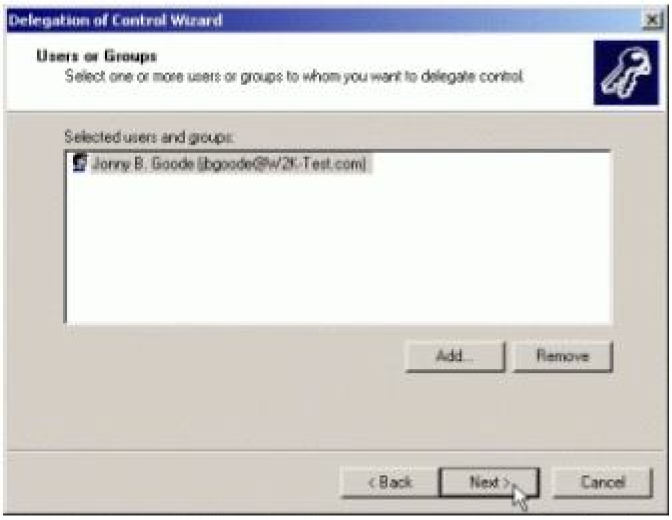
Look in: W2K-Test.com

Name	In Folder
Administrators	W2K-Test.com/Builtin
Users	W2K-Test.com/Builtin
Guests	W2K-Test.com/Builtin
Backup Operators	W2K-Test.com/Builtin
Replicator	W2K-Test.com/Builtin
Server Operators	W2K-Test.com/Builtin
Account Operators	W2K-Test.com/Builtin

<< Type names separated by semicolons or choose from list >>

Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Delegation of Control Wizard
Select Users, Computers, or Groups
Description
Selected
Add
Check Names
OK
Cancel

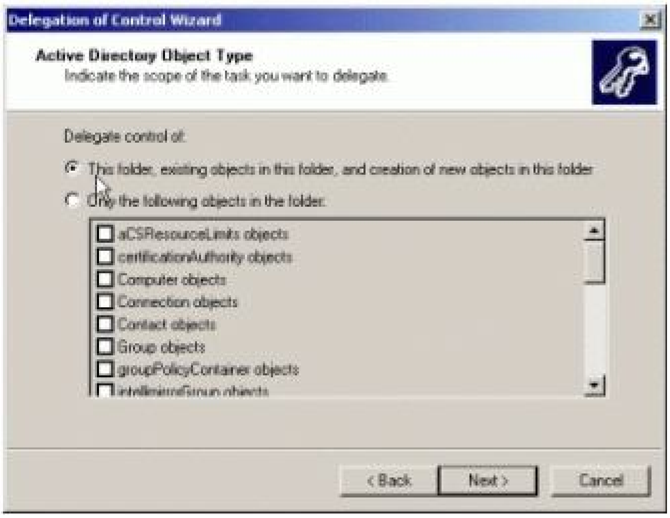
6. Select a user or group account, click **Add**, and click **OK**.



Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:
Jonny B. Goode (jbgoode@W2K-Test.com)

7. The next window provides two options for defining the scope of delegation. The first option, **This folder, existing objects in folder, and creation of new objects in this folder**, allows delegation of full control. The second option, **Only the following objects in the folder**, opens a selection window that allows administrators to specify the level of control they want to delegate.



Active Directory Object Type

Indicate the scope of the task you want to delegate.

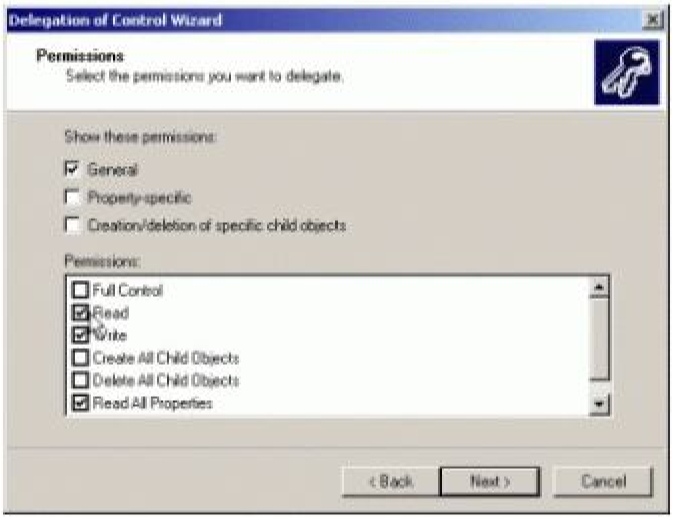
Delegate control of:

● This folder, existing objects in this folder, and creation of new objects in this folder

○ Only the following objects in the folder:

□ aCSResourceLimits objects
□ certificationAuthority objects
□ Computer objects
□ Connection objects
□ Contact objects
□ Group objects
□ groupPolicyContainer objects
□ intellimirrorGroup objects

8. Make a selection and click **Next**. The next window allows for the specifications of the permissions to delegate. Select the permissions to delegate and click **Next**



Permissions

Select the permissions you want to delegate.

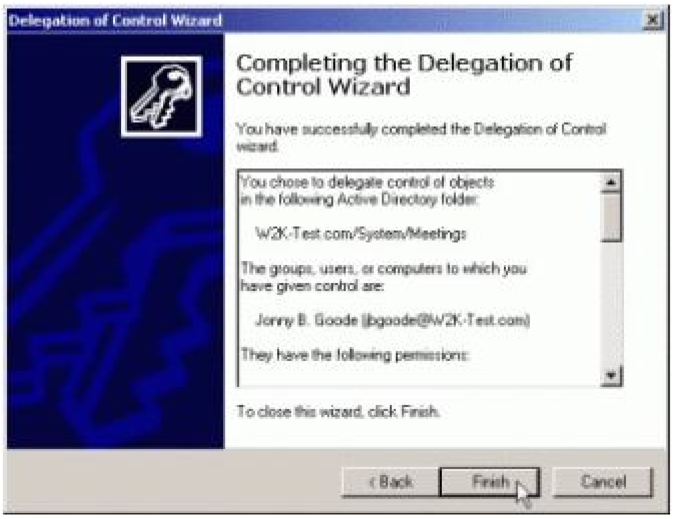
Show these permissions:

☑ General
□ Property-specific
□ Creation/deletion of specific child objects

Permissions:

□ Full Control
☑ Read
☑ Write
□ Create All Child Objects
□ Delete All Child Objects
☑ Read All Properties

9. A completion window will appear describing the selections. Click the **Finish** button.



Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

You chose to delegate control of objects in the following Active Directory folder:

W2K-Test.com/System/Meetings

The groups, users, or computers to which you have given control are:

Jonny B. Goode (jbgoode@W2K-Test.com)

They have the following permissions:

To close this wizard, click Finish.

Top Of Page