

Contents for File Security Help



Introduction

 [File Security Overview](#)

How To...

 [View or Set Permissions](#)

 [View or Set Auditing Information](#)

 [View or Take Ownership](#)




Contents for File Security Help



Introduction

-  [File Security Overview](#)
-  [What Is File Security?](#)
-  [Accessing File Security Properties](#)

How To...

-  [View or Set Permissions](#)
-  [View or Set Auditing Information](#)
-  [View or Take Ownership](#)







Contents for File Security Help



Introduction

 [File Security Overview](#)

How To...

-  [View or Set Permissions](#)
-  [Setting Directory Permissions](#)
-  [Setting File Permissions](#)
-  [Setting Special Access Permissions](#)
-  [View or Set Auditing Information](#)
-  [View or Take Ownership](#)

Contents for File Security Help



Introduction

- [File Security Overview](#)

How To...

- [View or Set Permissions](#)
- [View or Set Auditing Information](#)
- [Auditing Files and Directories](#)
- [Adding Users and Groups to Permissions and Auditing Lists](#)
- [View or Take Ownership](#)

Contents for File Security Help



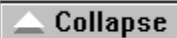
Introduction

- [File Security Overview](#)

How To...

- [View or Set Permissions](#)
- [View or Set Auditing Information](#)
- [View or Take Ownership](#)
- [Taking Ownership of Files or Directories](#)

Contents for File Security Help

 Collapse

Introduction


- [File Security Overview](#)
- [What Is File Security?](#)
- [Accessing File Security Properties](#)

How To...

- [View or Set Permissions](#)
- [Setting Directory Permissions](#)
- [Setting File Permissions](#)
- [Setting Special Access Permissions](#)
- [View or Set Auditing Information](#)
- [Auditing Files and Directories](#)
- [Adding Users and Groups to Permissions and Auditing Lists](#)
- [View or Take Ownership](#)
- [Taking Ownership of Files or Directories](#)

What Is File Security?

Files and directories on a computer running Windows NT Server or Windows NT Workstation can be protected with special security attributes. When you install Windows NT Server Tools on your Windows 95 computer, you can view these security attributes over the network and change them.

 To use any of the Windows NT Server Tools, you must have administrative privileges at the computer you choose to administer.

You can also use Server Manager to administer files and directories on a computer running Windows NT Server or Windows NT Workstation. Use Server Manager to share directories, set "share permissions" on shared directories (as opposed to permissions on files and directories themselves), see who is using shared resources, disconnect users from shared resources, and perform other tasks.


To return to Contents for File Security Help, click the Contents button.

See Also

[Accessing File Security Properties](#)

Accessing File Security Properties

The file or directory you want to administer must be on an NTFS-formatted drive of a computer running Windows NT Server or Windows NT Workstation.

 To change the properties of a shared file or directory, you must be logged on as a member of the Administrators, Server Operators, or Power Users group for the computer/domain you want to administer. Members of the Administrators group can change share properties on administrative shares, for example C\$.

To edit security properties of a file or directory

1. Focus on the file or directory and look at its Properties dialog box. There are many ways to do this. For example:
 - Click Start, point at Programs, and then click Windows Explorer. In the left pane, double-click Network Neighborhood. In the right pane, double-click the name of the computer you want to administer. In the right pane again, click the object you want to administer. Click the Properties button on the toolbar.
 - or -
 - Click Start, point at Find, and then click Computer. Type the name of the computer and then click Find Now. Double-click on the name of the computer. Click the object you want to administer. Click the Properties button on the toolbar.
 - or -
 - Use either method to specify the computer you want to administer. Click a set of objects you want to administer (for example, press the CTRL key on the keyboard while clicking more than one object). Click the Properties button on the toolbar to view or change properties for all of the objects at once.
2. In the Properties dialog box, click the Security tab. Now you can change the settings for permissions, auditing, and ownership of the object or set of objects.
3. For more information about changing security settings, see Windows NT Server documentation or the online Help.

NOTE: The following methods for selecting an object to administer do NOT work:

- Administering print queues through the Printers list in My Computer. These print queue objects represent print queues local to your Windows 95 computer, even if the queue is redirected to a Windows NT Server or Windows NT Workstation print queue.
- Using the Windows 3.x Print Manager. It no longer exists in Windows 95; the Printers icon in the Main group of Program Manager is just a shortcut to the Printers list in My Computer.
- Using File Manager (WINFILE.EXE) in Program Manager. Installing Windows NT Server Tools does not add a Security menu to File Manager as it did for Windows 3.x.

See Also

[What is File Security?](#)

Setting Directory Permissions

Setting permissions on a directory specifies the access that a group or user has to the directory and, by default, its files. Existing subdirectories and their files are not changed unless you specify to change them. However, when you create new files and subdirectories in the directory, they inherit their permissions from the directory.

Permissions are cumulative except that the No Access permission overrides all other permissions. For example, if a user is a member of a group with Read permission and a member of a group with Change permission, the user will have Change permission.

Note: Groups or users granted Full Control permission on a directory can delete files in that directory no matter what permissions protect the files.

You can set directory permissions only on drives formatted to use the Windows NT file system (NTFS).

To change permissions on the directory, you must be the owner of the directory, or have been granted permission to do so by the owner.

To view or change directory permissions

1. Select the directory in the Windows Explorer. You can select multiple directories.
2. Click the Properties button on the Windows Explorer Toolbar, then select the Security tab of the Properties dialog box.
3. Click Permissions.
4. By default, the Replace Permissions On Existing Files check box is selected, so the changes you make to permissions apply to the directory and its files only.

Select both the Replace Permissions On Subdirectories and the Replace Permissions On Existing Files check boxes to apply changed permissions to the directory and its files, and to existing subdirectories and their files.

To apply changed permissions to the directory only (not to existing files in the directory or to subdirectories and their existing files), clear both the Replace Permissions On Subdirectories and Replace Permissions On Existing Files check boxes.

To apply changed permissions to the directory and subdirectories only (not to existing files in the directory or subdirectories), select the Replace Permissions on Subdirectories check box and clear the Replace Permissions on Existing Files check box.

5. Select the name of a group or user and choose a permission from the Type of Access box.

You can customize directory and file permissions by choosing Special Directory Access... or Special File Access....

6. Click OK.

To remove directory permissions

▶ To remove directory permissions, select the name of the group or user in the Directory Permissions dialog box. Click Remove.

For help with any dialog box, click Help, or press F1 while using the dialog box.

See Also

Accessing File Security Properties

Directory Access Permissions

Adding Users and Groups to Permissions and Auditing Lists

Setting File Permissions

Setting permissions on a file specifies the access that a group or user has to it. When a file is created in a directory, it inherits its permissions from the directory.

Permissions are cumulative except that the No Access permission overrides all other permissions. For example, if a user is a member of a group with Read permission and a member of a group with Change permission, the user will have Change permission.

When you set a standard permission, a set of individual permissions is displayed next to it. For example, when you set Read permission on a file, you see (RX), signifying Read and Execute permissions on the file.

Note: Groups or users granted Full Control permission on the directory containing a file can delete the file no matter what permissions protect it.

You can set file permissions only on drives formatted to use the Windows NT file system (NTFS).

To change permissions on the file, you must be the owner of the file, or have been granted permission to do so by the owner.

To change permissions on a file

1. Select the file in the Windows Explorer. You can select multiple files.
2. Click the Properties button on the Windows Explorer Toolbar, then select the Security tab of the Properties dialog box.
3. Click Permissions.
4. In the File Permissions dialog box, select the name of the group or user whose permission you want to change.
5. Choose a permission from the Type of Access box.

To customize the permissions set for the group or user, choose Special Access... from the Type of Access box.

6. Click OK.

To remove file permissions

▶ To remove file permissions, select the name of the group or user in the File Permissions dialog box. Click Remove.

For help with any dialog box, click Help, or press F1 while using the dialog box.

See Also

[Accessing File Security Properties](#)

[File Access Permissions](#)

[Adding Users and Groups to Permissions and Auditing Lists](#)

Setting Special Access Permissions

In general, the standard directory and file permissions are all you need to secure your directories and files. However, if you want to create a custom set of permissions, you can use special access permissions. You can set special access permissions on directories, on all the files in selected directories, or on selected files.

When you set special access permissions on a directory, the permissions affect the directory only. Current permissions on files in the directory are not affected.

To set special access permissions

1. Select the file or directory in the Windows Explorer. You can select multiple files or multiple directories.
2. Click the Properties button on the Windows Explorer Toolbar, then select the Security tab of the Properties dialog box.
3. Click Permissions.
4. In the Permissions dialog box, select the group or user you want to grant special access.
5. Open the appropriate Special Access dialog box:

To set permissions on directories, choose Special Directory Access from the Type of Access box or double-click the name of the group or user.

To set permissions on all the files in the selected directories, choose Special File Access from the Type of Access box.

To set permissions on selected files, choose Special File Access from the Type of Access box or double-click the name of the group or user.

The Special Access dialog box shows which access permissions have been granted based on the current standard or special permissions setting.

6. To set special access permissions, select the check boxes for the access you want to grant.

To grant full control, select Full Control (All).

If you are setting permissions for all files in directories, you can select Access Not Specified. This removes permissions from files in the selected directories and prevents files from inheriting permissions from their directories.

7. Click OK.

For help with any dialog box, click Help, or press F1 while using the dialog box.

See Also

[Special Access Directory Permissions](#)

[Special Access File Permissions](#)

Auditing Files and Directories

Auditing files and directories allows you to track their usage. For a particular file or directory, you can specify which groups or users and which actions to audit. You can audit both successful and failed actions. Windows NT stores the information generated from auditing in a file. You can view the information using Event Viewer.

To audit files and directories, you must set the audit policy to audit file and object access. Set the audit policy using User Manager.

To audit files and directories, you must be logged on as a member of the Administrators group.

To audit a file or directory

1. Select the file or directory in the Windows Explorer. You can select multiple files or multiple directories.
2. Click the Properties button on the Windows Explorer Toolbar, then select the Security tab of the Properties dialog box.
3. Click Auditing.
4. If you are setting auditing on a directory, two check boxes allow you to control how auditing changes apply to existing files and subdirectories.

By default, the Replace Auditing On Existing Files check box is selected, so the changes you make to auditing apply to the directory and its files only.

Select both the Replace Auditing On Subdirectories and the Replace Auditing On Existing Files check boxes to apply auditing changes to the directory and its files, and to existing subdirectories and their files.

To apply auditing changes to the directory only (not to existing files in the directory or to subdirectories and their existing files), clear both the Replace Auditing On Subdirectories and Replace Auditing On Existing Files check boxes.

To apply auditing changes to the directory and subdirectories only (not to existing files in the directory or subdirectories), select the Replace Auditing on Subdirectories check box and clear the Replace Auditing on Existing Files check box.

5. Set auditing for each group or user in the list:

Select the name of a group or user, and then select the events to audit for that group or user.

6. Click OK.

To remove file or directory auditing for a group or user

1. In the Auditing dialog box, select the name of the group or user in the list.
2. Click Remove.

For help with any dialog box, click Help, or press F1 while using the dialog box.

See Also

[Audited Directory Events](#)

[Audited File Events](#)

Adding Users and Groups to Permissions and Auditing Lists

Adding Users and Groups to Permissions and Auditing Lists

The Add Users And Groups dialog box is available from the dialog boxes that allow you to change and remove permissions and auditing for users and groups. Use the dialog box to add users and groups to the permissions or auditing list, search for the members of a group, and find the domain to which a group or user belongs.

The Add Users And Groups dialog box displays the groups on the computer or in the domain shown by the List Names From box. Local groups are shown for the computer or domain whose name is followed by an asterisk (*). You can select another domain by using the List Names From box.

Domains appear only if your computer is a member of a domain on a Windows NT Server network. The domains shown have a trust relationship.

To add a user or group to a permissions or auditing list

1. In either the Directory Permissions or the Directory Auditing dialog box, click Add.

2. You can use options in the Add Users And Groups dialog box to display users, find the users in a group, or find the domain to which a group or user belongs.

To display the names of users on the selected computer or domain, click Show Users.

To see a group's content, select the group and click Members. Users are listed in a new dialog box. On a Windows NT Server network, global groups that are members of a local group appear in the list. To see a global group's users, select the group and click Members. To include the group in the Add Users And Groups dialog box, click Add. To include some of the group's users, select them and click Add.

To add a group or user, you must know the domain which contains the group's or user's account. On a Windows NT Server network, click Search to find the domain of a group or user. In the Find Account dialog box, type the name of the group or user in the Find User Or Group box and specify the domains you want to search. Then click Search. To include the groups or users in the Add Users And Groups dialog box, select them in the Search Results box and click Add.

3. To add groups or users to the list, select them in the Names box and click Add, or double-click the name of the group or user. Or you can type the names of groups and users in the Add Names box. Separate names using a semicolon.

If the account of the group or user is not located on the computer or domain shown by the List Names From box, you must specify the location. Type the computer or domain name followed by the group or user name and separate the names using a backslash—for example, SHIPPING\ERNESTA. You can type the name without waiting for Windows NT to list groups in the Names box.

4. If you are adding users or groups to a permissions list, select the permission for the groups or users shown in the Add Names box using the Type of Access box.

5. Click OK.

For help with any dialog box, click Help, or press F1 while using the dialog box.

Taking Ownership of Files or Directories

When you create a file or directory, you become the owner of it. By granting permissions, the owner controls how the file or directory is used. The owner can grant permission to another user to take ownership of a file or directory. Otherwise, you must be logged on as a member of the Administrators group to take ownership.

Although an administrator can take ownership, an administrator cannot transfer ownership to others. This preserves security. For example, only an administrator who takes ownership and changes permissions can gain access to a file on which you have set No Access permission. By checking the ownership of the file, you would see the ownership change and know who had violated the permission you set on the file. To make sure that your files are secure, you should check their ownership regularly.

To take ownership of a file or directory

1. Select the file or directory in the Windows Explorer. You can select multiple files or multiple directories.
2. Click the Properties button on the Windows Explorer Toolbar, then select the Security tab of the Properties dialog box.
3. Click Ownership.
4. Click Take Ownership.

If you have selected one or more directories, you can now specify whether you want to take ownership of all files and subdirectories in the trees of the selected directories. Click Yes if you want to do so.

For help with the Owner dialog box, click the Help button, or press F1 while using the dialog box.

Directory Access Permissions

When you set a directory permission, two sets of abbreviations for individual permissions are displayed next to it: The permissions set on the directory and the permissions set on files in the directory. For example, when you set Add & Read permission on a directory, you see (RWX), signifying Read, Write, and Execute permissions on the directory, and (RX) signifying Read and Execute permission on files in the directory.

When access to files is shown as (Not Specified), that group or user cannot use files in the directory unless access is granted by another means; for example, by setting permissions that grant access on individual files.

An asterisk (*) following the set of directory permissions, for example (All)*, indicates that subdirectories do not inherit the permissions granted to that group or user.

Note: Groups or users granted Full Control permission on a directory can delete files in that directory no matter what permissions protect the files.

You can set the following standard permissions on directories:

- No Access (None)(None)
- List (RX)(Not Specified)
- Read (RX)(RX)
- Add (WX)(Not Specified)
- Add & Read (RWX)(RX)
- Change (RWXD)(RWXD)
- Full Control (All)(All)

File Access Permissions

When you set a file permission, a set of abbreviations for individual permissions is displayed next to it. For example, when you set Read permission on a file, you see (RX) signifying Read and Execute permission.

Note: Groups or users granted Full Control permission on the directory containing a file can delete the file no matter what permissions protect it.

You can set the following standard permissions on files:

- No Access (None)
- Read (RX)
- Change (RWXD)
- Full Control (All)

Special Access Directory Permissions

You can set the following individual directory permissions when creating special access permission for directories:

Read (R)

Allows viewing the names of files and subdirectories.

Write (W)

Allows adding files and subdirectories.

Execute (X)

Allows changing to subdirectories in the directory.

Delete (D)

Allows deleting the directory.

Change Permissions (P)

Allows changing the directory's permissions.

Take Ownership (O)

Allows taking ownership of the directory.

Special Access File Permissions

You can set the following individual file permissions when creating special access permission for files:

Read (R)

Allows viewing the file's data.

Write (W)

Allows changing the file's data.

Execute (X)

Allows running the file if it is a program file.

Delete (D)

Allows deleting the file.

Change Permissions (P)

Allows changing the file's permissions.

Take Ownership (O)

Allows taking ownership of the file.

Shared Directory Permissions

You can set the following permissions for files and directories through a shared directory:

- No Access (None)
- Read
- Change
- Full Control (All)

Audited Directory Events

You can select the following events to audit directory actions:

Read

Audits display of filenames, attributes, permissions, and owner.

Write

Audits creation of subdirectories and files, changes to attributes, and display of permissions and owner.

Execute

Audits display of attributes, permissions, and owner; and changing to subdirectories.

Delete

Audits deletion of the directory.

Change Permissions

Audits changes to directory permissions.

Take Ownership

Audits changes to directory ownership.

Audited File Events

You can select the following events to audit file actions:

Read

Audits display of the file's data, attributes, permissions, and owner.

Write

Audits changes to the file's data or attributes, and display of permissions and owner.

Execute

Audits running of program files and display of attributes, permissions, and owner.

Delete

Audits deletion of the file.

Change Permissions

Audits changes to the file's permissions.

Take Ownership

Audits changes to the file's ownership.

Setting File Attributes

You can change the properties of a file. These properties include file attributes such as read only, archive, hidden, and system. File attributes are part of the directory information the operation system maintains for each file. This information helps the operating system identify a file and controls the kinds of tasks you can perform with the file. You can see file attributes in a directory window by choosing the All File Details command on the View menu.

On drives formatted to use the Windows NT file system (NTFS), you must have permission to change file attributes.

To change file attributes for one or more files

1. Select the files whose attributes you want to set.
2. From the File menu, choose Properties.

If you are using a network, more options may be available in the Properties dialog box.

3. In the Properties dialog box, select or clear the check boxes for the attribute settings.

When you select more than one file, check boxes appear gray if the attribute for the files is not set alike.

4. Click OK.

For help with the Properties dialog box, click Help, or press F1 while using the dialog box.

See Also

[Setting File Permissions](#)

Properties

Sets file attributes and displays other file information.

Click one of the following buttons for information about the dialog box:

- [Read Only](#)
- [Archive](#)
- [Hidden](#)
- [System](#)
- [Version Information](#)
- [Open By Button](#)

See Also

[Setting File Attributes](#)

Properties

Sets file attributes and displays information about the number and size of files selected.

Each option box has one of three settings:

- Attribute is set for all selected files.
- Attribute is not set for any of the selected files.
- Attribute is set for some, but not all, of the selected files.

Click one of the following buttons for information about a particular file attribute:

- [Read Only](#)
- [Archive](#)
- [Hidden](#)
- [System](#)

See Also

[Setting File Attributes](#)

Network Properties

Allows you to stop the use of a file and displays the status of a shared file, including the following information:

- Total Opens shows the total number of open files (including files open more than once) on the computer that the file is on.
- Total Locks shows the total number of locks on the computer that the file is on.
- Open By shows the names of the users who have the file open.
- For shows the type of access the user has to the file.
- Locks shows the number of locks the user has on the file.
- File ID shows the identification number of the file.

Caution

When you close a file that is in use, changes made to that file will not be saved.

- To stop the use of shared files, you must be logged on as a member of the Administrators, Server Operators, or Power Users group.

Close Selected

- To stop the use of a file by one or more users, select the users and click Close Selected.

Close All

- To stop the use of a file by all users, click Close All.

Owner

Displays the owner of the selected file or directory.

To take ownership of the file or directory, click Take Ownership.

See Also

[Taking Ownership of Files or Directories](#)

Add Users and Groups

Use the Add Users And Groups dialog box to add a group or user to the permission list for a file or directory.

Click one of the following buttons for information about the dialog box:

- [List Names From](#)
- [Names](#)
- [Add Button](#)
- [Show Users Button](#)
- [Members Button](#)
- [Search Button](#)
- [Add Names](#)
- [Type of Access](#)

See Also

[Adding Users and Groups to Permissions and Auditing Lists](#)

Local Group Membership

Displays the members of the local group selected in the Add Users And Groups dialog box.

To include the group in the Add Names box in the Add Users And Groups dialog box, click Add.

To include some of the listed members in the Add Names box in the Add Users And Groups dialog box, select them and click Add.

On a Windows NT Server network, global groups that are members of a local group appear in the list.

To see a global group's members, select the group and click Members.

See Also

[Adding Users and Groups to Permissions and Auditing Lists](#)

Global Group Membership

Displays the members of the global group selected in the Add Users And Groups dialog box or in the Local Group Membership dialog box.

- To include the group in the Add Names box in the Add Users And Groups dialog box, click Add.
- To include some of the listed members in the Add Names box in the Add Users And Groups dialog box, select them and click Add.

See Also

[Adding Users and Groups to Permissions and Auditing Lists](#)

Find Account

When you add a user or group to the permissions or audit list, you must know the name of the domain that contains the user or group's account. Use the Find Account dialog box to locate the domain of an account on a Windows NT Server network.

Click one of the following buttons for information about the dialog box:

[Find User or Group](#)

[Search All](#)

[Search Only In](#)

[Search Button](#)

[Add Button](#)

See Also

[Adding Users and Groups to Permissions and Auditing Lists](#)

File Permissions

Use the File Permissions dialog box to set or change permission for groups and users.

Click one of the following buttons for information about the dialog box:

- [File](#)
- [Owner](#)
- [Name](#)
- [Type of Access](#)
- [Add Button](#)
- [Remove Button](#)

See Also

[Setting File Permissions](#)

[File Access Permissions](#)

[Adding Users and Groups to Permissions and Auditing Lists](#)

Directory Permissions

Use the Directory Permissions dialog box to set or change permission for groups and users.

Click one of the following buttons for information about the dialog box:

- [Directory](#)
- [Owner](#)
- [Replace Permissions on Subdirectories](#)
- [Replace Permissions on Existing Files](#)
- [Name](#)
- [Type of Access](#)
- [Add Button](#)
- [Remove Button](#)

See Also

[Setting Directory Permissions](#)

[Directory Access Permissions](#)

[Adding Users and Groups to Permissions and Auditing Lists](#)

File or Directory Permissions

Sets file or directory permissions. When a file is selected, displays the File Permissions dialog box. When a directory is selected, displays the Directory Permissions dialog box.

See Also

[Directory Permissions](#)

[File Permissions](#)

Special Access File Permissions

Use the Special Access dialog box to set special access permission for a group or user.

Click one of the following buttons for information about the dialog box:

- [File](#)
- [Name](#)
- [Full Control \(All\)](#)
- [Other](#)

See Also

[Setting Special Access Permissions](#)

[Special Access File Permissions](#)

Special Directory Access

Use the Special Directory Access dialog box to set special access permission for a group or user.

Click one of the following buttons for information about the dialog box:

- [Directory](#)
- [Name](#)
- [Full Control \(All\)](#)
- [Other](#)

See Also

[Setting Special Access Permissions](#)

[Special Access Directory Permissions](#)

Special File Access

Use the Special File Access dialog box to set special access permissions for a group or user.

Click one of the following buttons for information about the dialog box:

- [Directory](#)
- [Name](#)
- [Access Not Specified](#)
- [Full Control \(All\)](#)
- [Other](#)

See Also

[Setting Special Access Permissions](#)

[Special Access File Permissions](#)

File Auditing

Use the File Auditing dialog box to audit the use of a file by groups and users. Click one of the following buttons for information about the dialog box:

- [File](#)
- [Name](#)
- [Events to Audit](#)
- [Add Button](#)
- [Remove Button](#)

See Also

[Auditing Files and Directories](#)

[Audited File Events](#)

[Adding Users and Groups to Permissions and Auditing Lists](#)

Directory Auditing

Use the Directory Auditing dialog box to audit the use of a directory by groups and users. Click one of the following buttons for information about the dialog box:

- [Directory](#)
- [Replace Auditing on Subdirectories](#)
- [Replace Auditing on Existing Files](#)
- [Name](#)
- [Events to Audit](#)
- [Add Button](#)
- [Remove Button](#)

See Also

[Auditing Files and Directories](#)

[Audited Directory Events](#)

[Adding Users and Groups to Permissions and Auditing Lists](#)

Add Users and Groups

Use the Add Users And Groups dialog box to add a group or user to the auditing list for a file or directory.

Click one of the following buttons for information about the dialog box:

- [List Names From](#)
- [Names](#)
- [Add Button](#)
- [Show Users Button](#)
- [Members Button](#)
- [Search Button](#)
- [Names](#)

See Also

[Adding Users and Groups to Permissions and Auditing Lists](#)

Add

Use the Add dialog box to add a group or user to the permission list for a file or directory.

Click one of the following buttons for information about the dialog box:

File or Directory

Name

Type of Access

File Permissions [LAN Manager 2.x]

Use the File Permissions dialog box to set or change permission for groups and users.

Click one of the following buttons for information about the dialog box:

- File
- Name
- Type of Access
- Add Button
- Remove Button

Directory Permissions [LAN Manager 2.x]

Use the Directory Permissions dialog box to set or change permission for groups and users.

Click one of the following buttons for information about the dialog box:

- [Directory](#)
- [Replace Permissions on Files/Subdirectories](#)
- [Name](#)
- [Type of Access](#)
- [Add Button](#)
- [Remove Button](#)

Special Access

Use the Special Access dialog box to set special access permission for a group or user.

Click one of the following buttons for information about the dialog box:

[File](#)

[Name](#)

[Permissions](#)

Special Directory Access

Use the Special Access dialog box to set special access permission for a group or user.

Click one of the following buttons for information about the dialog box:

- [Directory](#)
- [Name](#)
- [Permissions](#)

File Auditing [LAN Manager 2.x]

Use the File Auditing dialog box to audit the use of a file. Click one of the following buttons for information about the dialog box:

File

Events to Audit

Directory Auditing [LAN Manager 2.x]

Use the Directory Auditing dialog box to audit the use of a file. Click one of the following buttons for information about the dialog box:

- Directory
- Replace Auditing on Files/Subdirectories
- Events to Audit

Contents

Starts Help and displays the topics in File Security Help.

Search for Help on

Opens the Search dialog box for File Security Help. Using the Search dialog box, you can look up Help information by using keywords.

How to Use Help

Describes how to use Help.

About File Security

Displays version, mode, and copyright information about Windows.

Control Menu

The Control menu contains the following commands:

Restore

Restores the window to its former size after it has been maximized or minimized.

Move

Enables you to use the keyboard to move the window to another position.

Size

Enables you to use the keyboard to change the size of the window.

Minimize

Reduces the window to an icon.

Maximize

Enlarges the window to its maximum size.

Close

Quits an application, or closes a window or dialog box.

Next

Switches to the next window or icon.

Control Menu

The Control menu contains the following commands:

Restore

Restores the window to its former size after it has been maximized or minimized.

Move

Enables you to use the keyboard to move the window to another position.

Size

Enables you to use the keyboard to change the size of the window.

Minimize

Reduces the window to an icon.

Maximize

Enlarges the window to its maximum size.

Close

Quits an application, or closes a window or dialog box.

Switch To

Starts Task List, which you can use to switch between running applications and to rearrange their windows and icons.

Read Only

Select this check box if you want to prevent a file from being changed.

Archive

Select this check box if you want to mark a file that has changed since it was last backed up.

You may want to set the archive attribute if you use the Windows NT **backup** or **restore** command.

Hidden

Select this check box if you don't want a particular file to appear in a directory window.

If you want to display a file that has the hidden attribute set, you can choose By File Type from the View menu and then select the Show Hidden/System Files check box.

System

Select this check box if you want to identify a file as a system file.

When you select this check box, the file does not appear in directory listings. If you want the file to appear in a directory window in File Manager, you can choose By File Type from the View menu and then select the Show Hidden/System Files check box.

Version Information

Shows version information for files.

Select the subject in the left box to display the information on the subject in the right box.

Open By

Shows who is using shared files and allows you to stop the use of a file.

Files with Extension

This box displays the filename extension of the selected file.

To associate a file that has a different extension, type the extension in this box.


Associate With

From the Associate With list, select the file type and program that you want to associate with the extension shown in the Files With Extension box.


If the application you want to associate is not shown in the Associate With list, type the program filename including its extension in the Associate With box. You can use the Browse button to search for a program file.

To cancel an association, select (None) in the Associate With list.


Browse Button

 Click the Browse button to search for a program file.


New Type Button

-  Click this button to create a new file type that you can associate with a file extension.

Change Type Button

 Click this button to edit the file type selected in the Associate With list. You can also add and delete associations when you edit a file type.

Delete Type Button

 Click this button to delete the file type selected in the Associate With list.

File Type



Type a name for the file type.

File Type

To change the name of the file type, type another name in the File Type box.

Action

Choose the action, Open or Print, which executes the command in the Command box and the DDE options you specify.

Action

- Choose the action, Open or Print, whose command you want to change.

Command

Specifies the command for the action selected in the Action box.

- Type the name of the program file, including its extension, and any parameters. In commands, %1 represents the filename of the file currently selected in File Manager. If the application supports DDE, specify the name of the program file in the Command box and use the options in the DDE area to specify the DDE commands.

If the program is a Windows 3.1 application and you want it to run in a separate memory space from other Windows 3.1 applications, use the **cmd /c start /separate** *c:\apppath\appname.exe* syntax in the Command box (instead of just typing *c:\apppath\appname.exe*).


Command

You can change the commands for the file type. In commands, %1 represents the filename of the file currently selected in File Manager. If the application supports dynamic data exchange (DDE), specify the name of the program file in the Command box and use the options in the DDE area to specify the DDE commands.

To change the command for an action, choose the action in the Action box, and then edit the command in the Command box.

If the application is a Windows 3.1 application and you want it to run in a separate memory space from other Windows 3.1 applications, use the **cmd /c start /separate** *c:\appath\appname.exe* syntax in the Command box (instead of just typing *c:\appath\appname.exe*).

Browse Button

 Click this button to open a dialog box you can use to select a program file to use as a command.

Uses DDE

Specifies that the application uses DDE commands to perform the action.

DDE Message

Specifies the DDE command to use if the application is already running.

DDE Message Application Not Running

Specifies the DDE command to use if the application is not running.

Application

Specifies the DDE application string used to initiate a DDE conversation with the application specified in the Command box.

Topic

Specifies the DDE topic string used to initiate a DDE conversation with the application specified in the Command box.

Extensions Associated with this File Type

Use options in the Extensions Associated With This File Type area to add extensions to or remove extensions from the list of extensions associated with the file type shown in the File Type box.

- To add an extension, type the extension in the New Extension box and click Add.
- To remove an extension, select it in the Extensions box and click Remove.

File Name

Select a filename, and then click OK.

Or type a filename in this box, and then click OK. If the file is not in the current directory, include the path.

If the program file you want is not in the File Name list, you may have to change directories by choosing a directory in the Directories list.

List Files of Type

Open the list, and then select the type of file you want to appear in the File Name box.

Directories

Select the directory that contains the program file you want to use. The names of the files in that directory will appear in the File Name box.

If the directory you want is not in the list, you may have to change drives by opening the Drives list and selecting a drive.

Drives

- Open the list, and then select the drive that contains the program file you want. The directories on that drive will appear in the Directories box.

Share Name

Shows the name users specify to connect to the shared directory. In order for MS-DOS computers to connect, the name must conform to the MS-DOS 8.3 naming convention. On Windows NT networks, the name can be up to 12 characters long.

By default, the name is the name of the selected directory. You can type a different name in the Share Name box.

Share Name

Shows the name users specify to connect to the shared directory. You cannot change the share name of a shared directory; however, you can share the directory again under a different name.

If the directory has been shared more than once, you can select the share name of the share whose properties you want to change.

Path

Shows the path and name of the selected directory.

By default, the path is the path of the selected directory. To share a different directory, type the directory's path and name.

Path

Shows the path and name of the selected shared directory.

Comment

The optional comment is displayed with the share name in the Connect Network Drive dialog box.

Type a comment describing the shared directory.

Comment

Shows the comment for the currently selected share.

To change the comment, type the changes in the Comment box.

User Limit

Sets the maximum number of users who can connect to the shared directory at one time.
By default, no limit is set.

To set a limit, click Allow and set a limit in the Users box.

User Limit

Shows the user limit for the currently selected share.

- To set a limit, click Allow and set a limit in the Users box.
- To remove the limit, click Unlimited.


Permissions Button

You can control access to a shared directory by setting permissions on it.

 To secure the directory, click Permissions.

Permissions Button

Shows the permissions set on the currently selected share.

 To change the permissions set on the share, click Permissions.

List Names From

Displays the name of the domain or computer whose groups are shown in the Names box. An asterisk (*) following the name indicates that local groups for that domain or computer are shown.

To display groups and users in another domain or on the computer, select another domain or select the computer.

Names

Displays the groups or users belonging to the current domain or computer.

To add groups or users to the permissions list, select them in the Names box and click Add.

Names


Displays the groups or users belonging to the current domain or computer.

To add groups and users to the auditing list, select them in the Names box and click Add.

Add Button

- To add groups or users to the audit list, select them in the Names box and click Add.

Members Button

 To see a group's content, select the group in the Names box and click Members.

Search Button

To add a group or user, you must know the domain that contains the account for the group or user.

- To find the domain to which a group or user belongs, click Search.

Add Names

Displays the names of groups and users who you are adding to the audit list.

To add groups or users to the Add Names box, select them in the Names box and click Add.


Or type the names of groups and users in the Add Names box. Separate names with a semicolon. If the account of the group or user is not located on the computer or domain shown by the List Names From box, specify the location. Type the computer or domain name followed by the group or user name and separate the names with a backslash.

Name


Displays the groups and users on the current server.

To set a permission, select the group or user, and select a permission from the Type Of Access box. Then click OK.


Add Button

 To add groups or users to the permissions list, select them in the Names box and click Add.

Show Users Button

 To display the names of users belonging to the current domain or computer in the Names box, click Show Users.

Members Button

 To see a group's content, select the group in the Names box and click Members.

Search Button

To add a group or user, you must know the domain that contains the account for the group or user.

- To find the domain to which a group or user belongs, click Search.

Add Names

Displays the names of groups and users who you are adding to the permissions list.

To add groups or users to the Add Names box, select them in the Names box and click Add.

Or type the names of groups and users in the Add Names box. Separate names with a semicolon. If the account of the group or user is not located on the computer or domain shown by the List Names From box, specify the location. Type the computer or domain name followed by the group or user name and separate the names with a backslash.

Type of Access

Displays a list of available permissions.

To set a permission for the groups and users listed in the Add Names box, select a permission, and then click OK.

Type of Access

Displays a list of available permissions.

To set a permission, select the group or user from the Name box and select a permission, and then click OK.

File

Displays the path and name of the selected file.

Directory

Displays the name of the selected directory.

Access Through Share

Displays the name of the shared directory through which access to files and directories is controlled.

File or Directory

Displays the name of the selected file or directory.

Owner

Displays the name of the owner of the file.

Owner

Displays the name of the owner of the directory.

Owner

The name of the owner of a shared directory is not displayed. Ownership of a shared directory does not affect who can set permissions.

Replace Permissions on Subdirectories

By default, permissions you set apply only to the directory and its files.

Select the check box to apply permissions to all subdirectories. If the Replace Permissions on Existing Files check box is selected, permissions are changed on the files in subdirectories as well.

Replace Permissions on Existing Files

By default, permissions you set apply to files in the directory as well as to the directory itself.

Clear the check box to apply permissions to the directory only. If the Replace Permissions on Subdirectories check box is selected, permissions are changed on subdirectories as well.

Replace Permissions on Files/Subdirectories

Normally, permissions you set apply to the directory itself and to files that currently have no permissions set on them.

- Select the check box to apply permissions to all existing files and subdirectories.

Name

Displays the names of groups and users and their current permissions.

To change a permission, select the group or user and select a permission from the Type Of Access box.

Type of Access

Displays a list of available permissions.

To change a permission, select the group or user from the Name box and select a permission.

Type of Access

Displays a list of available permissions.

To change a permission, select the group or user from the Name box and select a permission.

Type of Access

Displays a list of available permissions.

To change a permission, select the group or user from the Name box and select a permission.

Type of Access

Displays a list of available permissions.

To change a permission, select the group or user from the Name box and select a permission.

Type of Access

Displays a list of available permissions.


To change a permission, select the group or user from the Name box and select a permission.

Type of Access


Displays a list of available permissions.

To set a permission, select the group or user from the Name box and select a permission, and then click OK.

Add Button

 To add groups or users to the permission list, click Add.

Remove Button

 To remove a group or user from the permission list, select the group or user, and then click Remove.

Find User or Group

In the Find User Or Group box, type the name of the group or user whose account you want to find.


Search All

To search for the account in all the listed domains, select the Search All button.


Search Only In

To search for the account in one or more domains, select them in the Search Only In box.

Search Button

 After specifying a group or user and the domains to search, click Search to start the search.

Add Button

 To add the user or group to the Add Names box in the Add Users And Groups dialog box, select the user or group in the Search Results box and then click Add.

File

Displays the path and name of the selected file.

Directory

Displays the name of the selected directory.

Share

Displays the share name of the selected share.

Name

Displays the name of the selected group or user.

Access Not Specified

Select the Access Not Specified button to prevent files from inheriting permissions from the directory.

Full Control (All)

- Select Full Control (All) to grant the selected group or user Full Control of the file.

Full Control (All)

Select Full Control (All) to grant the selected group or user Full Control of the directory.

Other

Select the check boxes for the access you want to grant.

Other

Select the check boxes for the access you want to grant.

Permissions

Select the check boxes for the access you want to grant.

Permissions

Select the check boxes for the access you want to grant.

Name

Displays the names of currently audited groups and users.

Replace Auditing on Subdirectories

By default, auditing changes apply only to the directory and its files.

Select the check box to apply auditing to all subdirectories. If the Replace Auditing on Existing Files check box is selected, auditing changes apply to the files in subdirectories as well.

Replace Auditing on Existing Files

By default, auditing changes apply to files in the directory as well as to the directory itself.

Clear the check box to apply auditing changes to the directory only. If the Replace Auditing on Subdirectories check box is selected, auditing changes apply to subdirectories as well.

Replace Auditing on Files/Subdirectories

Events you specify for auditing are audited for the directory itself and for files that are currently not audited.

Select the check box to apply auditing to all existing files and subdirectories whether or not they are currently audited.

Events to Audit

For a particular file, you can audit events that succeed and those that fail.

Select a group or user, and then select the events you want to audit for the file by selecting the appropriate check boxes.

Events to Audit

For a particular directory, you can audit events that succeed and those that fail.


Select a group or user, and then select the events you want to audit for the directory by selecting the appropriate check boxes.

Events to Audit


You can audit events that succeed and those that fail.

Select the events you want to audit by selecting the appropriate check boxes.

Add Button

 To add groups or users to the auditing list, click Add.

Remove Button

 To remove a group or user from the auditing list, select the group or user, and then click Remove.

Enter Network Password

You must supply a password to connect to the shared directory.

Type your password in the Password box and click OK.

Restoring Network Connections

For the reason shown in the Restoring Network Connections dialog box, a network connection has not been restored.

If you no longer want to restore this connection automatically, choose the Do Not Try To Restore The Connection In The Future check box.

Add Users And Groups

Use the Add Users And Groups dialog box to add a group or user to the permission list for the share.

Click one of the following buttons for information about the dialog box:

- [List Names From](#)
- [Names](#)
- [Add Button](#)
- [Show Users Button](#)
- [Members Button](#)
- [Search Button](#)
- [Add Names](#)
- [Type of Access](#)

See Also

[Adding Users and Groups to Permissions and Auditing Lists](#)

Share Properties

Use the Share Properties dialog box to change properties for a shared directory.

Click one of the following buttons for information about the dialog box:

- Share Name
- Path
- Comment
- User Limit
- Permissions Button

New Share

Shares the selected directory.

Click one of the following buttons for more information about the dialog box:

- [Share Name](#)
- [Path](#)
- [Comment](#)
- [User Limit](#)
- [Permissions Button](#)

Shared Directories

Allows you to create a new share, change share properties for a shared directory, or stop sharing a directory.

Click one of the following buttons for more information about the dialog box:

- [Shared Directories on](#)
- [New Share Button](#)
- [Properties Button](#)
- [Stop Sharing Button](#)

Enter Password (LAN Manager 2.x)

To perform administrative tasks on the server, you must supply a password.

- To connect to the server, type the password in the Password box and click OK.

Access Type -- Read Only

- To allow users to only read files and execute programs, select Read Only.

Access Type -- Change

To allow users to read files, execute programs, change files, create and delete files and subdirectories, and set attributes; select Change.

Access Type -- Other

To specify access using individual permissions, type the abbreviation for each permission in the Other box. R (read), W (write), X (execute), D (delete), C (create), A (set attributes), and P (set permissions).

Password

- To set a password that protects the directory, type the password in the Password box.

Share Name

Shows the share name of the selected shared directory.

Path

Shows the directory path for the currently selected share. By changing the path, you can change the directory you are sharing under the current share name.

To change the path, type the new path in the path box.

Comment

Shows the comment for the currently selected share.

To change the comment, type the changes in the Comment box.


User Limit

Shows the user limit for the currently selected share.

- To set a limit, click Allow and set a limit in the Users box.
- To remove the limit, click Unlimited.

Permissions Button

Shows the permissions set on the currently selected share.

 To change the permissions set on the share, click Permissions.

Share Name

The share name is the name users specify to connect to the shared directory. In order for MS-DOS computers to connect, the name must conform to the MS-DOS 8.3 naming convention. On Windows NT networks, the name can be 12 characters long.

Type a share name for the shared directory in the Share Name box.

Path

Type the path and name of the directory you want to share in the Path box.

Comment

The optional comment is displayed with the share name in the Connect Network Drive dialog box.

- Type a comment describing the shared directory in the Comment box.

User Limit

Sets the maximum number of users who can connect to the shared directory at one time.
By default, no limit is set.

To set a limit, click Allow and set a limit in the Users box.

Permissions Button

You can control access to a shared directory by setting permissions for groups and users on it.

To secure the directory, click Permissions.

Shared Directories on

Displays the shared directories on the selected computer.

New Share Button

Allows you to share a directory. Selecting an administrative share on the computer before choosing the New Share button allows you to share any directory on that drive. For example, selecting C\$ allows you to share directories on the C: drive.

Properties Button

Select the shared directory whose properties you want to change, and click Properties.

You can change the following properties for the selected share:

- The directory that is shared under that share name.
- The comment displayed with the share name.
- The number of users allowed to connect to the share at one time.
- Permissions controlling access to the share.

Stop Sharing Button

- Select the shared directory that you want to stop sharing and click Stop Sharing.

No Access (None)(None)

Prevents any access to the directory and its files. Specifying No Access for a user prevents access even if that user belongs to a group that has access to the directory.

List (RX)(Not Specified)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.

Does not allow:

- Access to files, unless granted by other directory or file permissions.

Read (RX)(RX)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running applications.

Add (WX)(Not Specified)

Allows:

- Adding files and subdirectories to the directory.

Does not allow:

- Access to files, unless granted by other directory or file permissions.

Add & Read (RWX)(RX)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory.

Change (RWXD)(RWXD)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory.
- Changing data in files.
- Deleting the directory and its files.

Full Control (All)(All)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory.
- Changing data in files.
- Deleting the directory and its files.
- Changing permissions on the directory and its files.
- Taking ownership of the directory and its files.

No Access (None)

Prevents any access to the file. Specifying No Access for a user prevents access even if that user belongs to a group that has access to the file.

Read (RX)

Allows:

- Viewing the file's data.
- Running the file if it is a program file.

Change (RWXD)

Allows:

- Viewing the file's data.
- Running the file if it is a program file.
- Changing data in the file.
- Deleting the file.

Full Control (All)

Allows:

- Viewing the file's data.
- Running the file if it is a program file.
- Changing data in the file.
- Deleting the file.
- Changing permissions on the file.
- Taking ownership of the file.

No Access (None)

Prevents any access to the shared directory, its subdirectories, and its files.

Read

Allows:

- Viewing filenames and subdirectory names.
- Changing to the shared directory's subdirectories.
- Viewing data in files and running application files.

Change

Allows:

- Viewing filenames and subdirectory names.
- Changing to the shared directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the shared directory.
- Changing data in files.
- Deleting subdirectories and files.

Full Control (All)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the shared directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the shared directory.
- Changing data in files.
- Deleting subdirectories and files.
- Changing permissions (NTFS files and directories only).
- Taking ownership (NTFS files and directories only).

associate

To identify a filename extension as "belonging" to a certain application, so that when you open any file with that extension, the application starts automatically.

attributes

Information that indicates whether a file is a read-only, hidden, or system file, and whether the file has been changed since a backup copy of it was made.

active

The window or icon that you are currently using or that is currently selected. Windows NT always applies the next keystroke or command you choose to the active window. If a window is active, its title bar changes color to differentiate it from other windows. If an icon is active, its label changes color.

Windows or icons on the desktop that are not selected are inactive.

branch

A segment of the directory tree, representing a directory and any subdirectories it contains.

collapse

To hide additional directory levels below a selected directory in the directory tree.

default printer

The printer that is used if you choose the Print command without first specifying which printer you want to use with an application. You can have only one default printer; it should be the printer you use most often.

directory tree

A graphical display of a disk's directory structure. The directories on the disk are shown as a branching structure. The top-level directory is the root directory.

directory window

A File Manager window that displays the contents of a disk. The window shows both the directory tree and the contents of the current directory.

document file

A file that is associated with an application. When you open a document file, the application starts and loads the file.

document-file icon

Represents a file that is associated with an application. When you choose a document-file icon, the application starts and loads the file.

drive icon

An icon that represents a disk drive on your system. Different icons depict floppy disk drives, hard disk drives, network drives, RAM drives, and CD-ROM drives.

expand

To show hidden directory levels in the directory tree. You can expand a single directory level, one branch of the directory tree, or all branches at once.

file allocation table (FAT)

A table or list maintained by some operating systems to keep track of the status of various segments of disk space used for file storage.

font

A graphic design applied to a collection of numbers, symbols, and characters. A font usually comes in different sizes and styles.

icon

A graphical representation of an element in Windows NT, such as a disk drive, directory, group, application, or document. You can enlarge an application icon to a window when you want to use the application.

path

Specifies the location of a file within the directory tree. For example, to specify the path of a file named README.WRI located in the WINDOWS directory on drive C, you would type **c:\windows\readme.wri**.

program file

A file that starts an application or program. A program file has an .EXE, .PIF, .COM, or .BAT filename extension.

reduce

To minimize a window to an icon by using the Minimize button or the Minimize command. A minimized application continues running, and you can select the icon to make it the active application.

status bar

A line of information related to the application in the window. Usually located at the bottom of a window. Not all windows have a status bar.

title bar

The horizontal bar (at the top of a window) that contains the title of the window or dialog box. On many windows, the title bar also contains the Control-menu box and Maximize and Minimize buttons.

wildcard

A character that represents one or more characters. The question mark (?) wildcard can be used to represent any single character, and the asterisk (*) wildcard can be used to represent any character or group of characters that might match that position in other filenames.

