Click **Help Topics** for a list of Help topics.

Click to set, view, change, or remove permissions for one or more files or directories.

Click to set, view, change, or remove auditing for one or more files or directories.

Click to take ownership of one or more files or directories.

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 the following for information about the dialog box:
□ List Names From
□ Names
□ Add
□ Show Users
□ Members
□ Search
□ Add Names

{button ,AL("a_add_aud")} Related Topics

List Names From

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

Names

Displays the groups (and users if **Show Users** is selected) whose accounts belong to the current domain or computer. You can add to the auditing list by selecting groups and users and clicking **Add**.

Add

Adds groups and users selected in **Names** to the auditing list.

Show Users

Displays the names of users belonging to the domain or computer selected in **List Names From**. By default, only groups are displayed.

Members

Displays the contents of the group selected in **Names**.

Search

Looks for the domain to which a selected user or group belongs. To add a group or user, you must know which domain contains the account before you can add it to the list.

Add Names

Displays the names of groups and users you are adding to the auditing list. You can include other users and groups by selecting them in **Names** and clicking **Add**.

Add Users and Groups

Used to add a group or user to the permissions list for a file or directory.

Click the following for information about the dialog box:

□ List Names From
□ Names
□ Add
□ Show Users
□ Members
□ Search
□ Add Names
□ Type of Access

{button ,AL("a_add_perm")} Related Topics

Names

Displays the groups(and users if **Show Users** is selected) belonging to the current domain or computer. You can add to the permissions list by selecting groups and users and clicking **Add**.

Add

Adds groups and users selected in **Names** to the permissions list.

Members

Displays the contents of the group selected in **Names**.

Search

Looks for the domain to which a selected user or group belongs. To add a group or user, you must know which domain contains the account before you can add it to the list.

Add Names

Displays the names of groups and users you are adding to the list. You can include other users and groups by selecting them in **Names** and clicking **Add**.

Type of Access

Displays a list of available permissions.

Find Account

If you don't 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 the following for information about the dialog box:

□ Find User or Group

□ Search All

□ Search Only In

□ Search

□ Add

{button ,AL("a_add_aud")} Related Topics

Find User or Group

Used to enter the name of the group or user whose account you want to find.

Search All

Sets the search to look for the account in all the listed domains.

Search Only In

Limits the search for the account to the selected domains.

Search

Starts the search for the specified group or user.

Add

Adds the selected user or group in **Search Results** to **Add Names** in the **Add Users and Groups** dialog box.

Directory Auditing

Used to audit the use of a directory by groups and users.

Click the following for information about this dialog box:
□ Directory
□ Replace Auditing on Subdirectories
□ Replace Auditing on Existing Files
□ Name
□ Events to Audit
□ Add
□ Remove

{button ,AL("a_audit_file_dir;a_add_aud;a_audit_dir_events")} Related Topics

Directory

Displays the name of the selected directory.

Replace Auditing on Subdirectories

When selected, applies auditing to all subdirectories in the selected directory and those subdirectory files. By default, this is not selected.

Replace Auditing on Existing Files

When selected, applies auditing to the selected directory and all files within it (the default setting). When this check box is cleared, auditing changes apply to the directory but not to its files.

Name

Displays the names of currently audited groups and users.

Events to Audit

Used to set auditing events to record successes, failures, both, or neither for selected users or groups.

Add

Adds groups or users to the auditing list.

Remove

Removes selected groups or users from the auditing list.

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 displays of permissions and owner.

Execute

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

Delete

Audits deletion of the directory.

Change Permissions

Audits changes to directory permissions.

Take Ownership

Audits changes to directory ownership.

File Auditing

Used to audit the use of a file by groups and users.

Click the following for information about this dialog box:

□ File
□ Name
□ Events to Audit
□ Add
□ Remove

{button ,AL("a_audit_file_events;a_add_aud;a_audit_file_dir")} Related Topics

File

Displays the path and name of the selected file.

Events to Audit

Used to set auditing events to record successes, failures, both, or neither for selected users or groups.

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 file permissions.

Take Ownership

Audits changes to file ownership.

Directory Permissions

Used to set or change permission for groups and users.

Click the following for information about this dialog box:

□ Directory
□ Owner
□ Replace Permissions on Subdirectories
□ Replace Permissions on Existing Files
□ Name
□ Type of Access
□ Add
□ Remove

{button ,AL("a_set_rem_dir_perm;a_dir_access_perm;a_add_perm")} Related Topics

Owner

Displays the name of the owner of the directory.

Replace Permissions on Subdirectories

When selected, replaces permissions for all subdirectories in the selected directory and those subdirectory files. By default, this is not selected.

Replace Permissions on Existing Files

When selected, changes permissions for the selected directory and all files within it (the default setting). when this check box is cleared, permission changes apply to the directory but not to its files.

Name

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

Type of Access

Displays a list of available permissions.

Add

Adds selected groups and users to the permission list.

Remove

Removes selected groups and users from the permission list.

Directory Access Permissions

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)

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.
- Making changes to subdirectories in the directory.

Does not allow:

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

Read (RX)(RX)

Allows:

- Viewing filenames and subdirectory names.
- Making changes to subdirectories in the directory.
- 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.
- Making changes to subdirectories in the directory.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory.

Change (RWXD)(RWXD)

Allows:

- Viewing filenames and subdirectory names.
- Making changes to subdirectories in the directory.
- 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.
- Making changes to subdirectories in the directory.
- 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.

File Permissions

Used to set or change permission for groups and users.

Click the following for information about this dialog box:
□ File
□ Owner
□ Name
□ Type of Access
□ Add
□ Remove

{button ,AL("a_set_rem_file_perm;a_file_access_perm;a_add_perm")} Related Topics

Owner

Displays the name of the owner of the file.

Type of Access

Displays a list of available permissions.

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 a 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)

{button ,AL("a_spec_access_perm;a_set_rem_file_perm")} Related Topics

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 data in a file.
- Running the file if it is a program file.

Change (RWXD)

Allows:

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

Full Control (All)

Allows:

- Viewing the data in a file.
- 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.

Special Access

Used to set special file-access permissions for a group or user.

Click the following for information about this dialog box:
□ File
□ Name
□ Full Control (All)
□ Other

{button ,AL("a_set_spec_access_perm;a_spec_file_perms")} Related Topics

File

Displays the path and name of the selected file, or the number of files if more than one is selected.

Name

Displays the name of the selected group or user.

Full Control (All)

When selected, grants all the special file-access permissions to the selected group or user.

Other

Displays check boxes for the specific permissions you can grant.

Special Directory Access

Used to set special directory-access permissions for a group or user.

Click the following for information about this dialog box:
□ Directory
□ Name
□ Full Control (All)
□ Other

{button ,AL("a_set_spec_access_perm;a_spec_dir_perms")} Related Topics

Directory

Displays the name of the selected directory.

Full Control (All)

When selected, grants all the special directory-access permissions to the selected group or user.

Other

Displays check boxes for the specific permissions you can grant.

Special File Access

Used to set special file-access permissions on all files in the selected directories for a group or user.

Click the following for information about this dialog box:
□ Directory
□ Name
□ Access Not Specified
□ Full Control (All)
□ Other

{button ,AL("a_set_spec_access_perm;a_spec_file_perms")} Related Topics

Access Not Specified

Prevents files from inheriting permissions from the directory.

Special Access Directory Permissions

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

Read (R)

Allows viewing filenames and subdirectory names.

Write (W)

Allows adding files and subdirectories.

Execute (X)

Allows changing to subdirectories in the directory.

Delete (D)

Allows deletion of the directory.

Change Permissions (P)

Allows changing the directory permissions.

Take Ownership (O)

Allows taking ownership of the directory.

{button ,AL("a_spec_access_perm")} Related Topics

Special Access File Permissions

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

Read (R)

Allows viewing data in the file.

Write (W)

Allows changing data in the file.

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 permissions.

Take Ownership (O)

Allows taking ownership of the file.

{button ,AL("a_spec_access_perm")} Related Topics

Local Group Membership

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

- To add the entire group membership to **Add Names** in the **Add Users and Groups** dialog box, click **Add**.

Or, to include only some of the listed members, select them, and then click **Add**.

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

- To see the members of a global group, select the group and then click **Members**.

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 **Add Names** in the **Add Users and Groups** dialog box, click **Add**.

Or, to include only some of the listed members, select them, and then click **Add**.

Owner

Displays the owner of the selected file or directory.

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

File Permissions [LAN Manager 2.x]

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

Click the following for information about this dialog box:

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

Type of Access

Displays a list of available permissions.

- To change a permission, select the group or user in **Name** and select a permission.

Directory Permissions [LAN Manager 2.x]

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

Click the following for information about this dialog box:

□ Directory
□ Replace Permissions on Files/Subdirectories
□ Name
□ Type of Access
□ Add Button
□ Remove Button

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.

Type of Access

Displays a list of available permissions.

- To change a permission, select the group or user in **Name** and select a permission.

Special Access

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

Click the following for information about this dialog box:

□ File

□ Name

□ Permissions

Permissions

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

Special Directory Access

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

Click the following for information about this dialog box:

□ Directory
□ Name
□ Permissions

Permissions

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

File Auditing [LAN Manager 2.x]

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

- □ File
- □ Events to Audit

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.

Directory Auditing [LAN Manager 2.x]

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

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

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.

To audit a file or directory

1 In My Computer, select the file or directory you want to audit.

2 On the **File** menu, click **Properties**.

3 Click the **Security** tab, and then click **Auditing**.

4 Set the level to which auditing changes will apply by doing one of the following:

- To affect only the directory and its files, select **Replace Auditing On Existing Files**.
- To affect the directory, its files, subdirectories, and subdirectory files, select both **Replace Auditing On Subdirectories** and **Replace Auditing On Existing Files**.
- To affect only the directory (not the files, subdirectories or subdirectory files), click to clear both **Replace Auditing On Subdirectories** and **Replace Auditing On Existing Files**.
- To affect only the directory and subdirectories (not files in the directory or subdirectories), select **Replace Auditing on Subdirectories** and click to clear **Replace Auditing on Existing Files**.

5 To add a user or group to **Name**, click **Add** and complete the **Add Users and Groups** dialog box.

6 Select one or more users or groups in **Names**.

7 Under **Events to Audit**, select **Success**, **Failure**, or both for each event you want to audit.

Note

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

{button ,AL("a_audit_file_dir_rem;a_add_aud")} Related Topics

To remove file- or directory-auditing for a group or user

1 In My Computer, select the file or directory for which you want to remove auditing.

2 On the **File** menu, click **Properties**.

3 Click the **Security** tab, and then click **Auditing**.

4 In **Name**, select the groups or users you want.

5 Click **Remove**.

To take ownership of files or directories

1 In My Computer, select one or more files or directories.

2 On the **File** menu, click **Properties**.

3 Click **Ownership**.

4 Click **Take Ownership**.

To add a user or group to an auditing list

1. In the **File Auditing** or **Directory Auditing** dialog box, click **Add**.
2. Select the users or groups in **Names**, and click **Add**.
3. If necessary, use **Names** to add accounts to the auditing list:

- To add an entire group, select it and click **Add**.
- To see a list of users on the selected computer or domain, click **Show Users**.
- To see the contents of a selected group, click **Members**.
- To add only some members of a group, select them in a **Group Membership** dialog box, and click **Add**.

Notes and Tips

- If you don't know the domain of the user or group, click **Search**.
- An asterisk (*) following the domain or computer name indicates that local groups for that domain or computer are shown. You can click another domain.
- 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.

{button ,AL("a_find_account")} Related Topics

To add a user or group to a permissions list

1 In the **Directory Permissions** or **File Permissions** dialog box, click **Add**.

2 Select the users and groups in **Names**, and click **Add**.

3 Select a permission in **Type of Access**.

4 If necessary, use **Names** to add accounts to the permission list:

- To add an entire group, select it and click **Add**.
- To see all the users on a selected computer or domain, click **Show Users**.
- To see the contents of a selected group, click **Members**.
- To add only some members of a group, select them in a **Group Membership** dialog box, and click **Add**.

Notes and Tips

- If you don't know the domain of the user or group, click **Search**.
- An asterisk (*) following the domain or computer name indicates that local groups for that domain or computer are shown. You can click another domain.
- 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 set, view, change, or remove directory permissions

1 In My Computer, select one or more directories.

2 On the **File** menu, click **Properties**.

3 Click the **Security** tab, and then click **Permissions**.

4 Set the level to which permission changes will apply by doing one of the following:

- To affect only the directory and its files, select **Replace Permissions On Existing Files**.
- To affect the directory, its files, subdirectories, and subdirectory files, select both **Replace Permissions On Subdirectories** and **Replace Permissions On Existing Files**.
- To affect only the directory (not the files, subdirectories or subdirectory files), click to clear both **Replace Permissions On Subdirectories** and **Replace Permissions On Existing Files**.
- To affect only the directory and subdirectories (not files in the directory or subdirectories), select **Replace Permissions on Subdirectories** and click to clear **Replace Permissions on Existing Files**.

4 To add a user or group to the permissions list, click **Add** and complete the **Add Users and Groups** dialog box.

5 In **Type of Access**, select a permission.

To remove directory permissions

- Select the group or user in the **Name** box and then click **Remove**.

Notes

- To customize permissions, select **Special Directory Access** or **Special File Access** in **Type of Access**.
- After you set permissions, new files and subdirectories you create in the directory inherit permissions from the directory.
- Groups or users granted Full Control permission for a directory can delete files in that directory no matter what permissions protect the files.
- 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.
- You can set directory permissions only on drives formatted to use the Windows NT file system (NTFS).

{button ,AL("a_dir_access_perm;a_add_perm;a_spec_access_perm")} Related Topics

To set, view, change, or remove file permissions

1 In My Computer, select one or more files and on the **File** menu, and click **Properties**.

2 Click the **Security** tab, and then click **Permissions**.

3 In the **File Permissions** dialog box, select the name of a group or user.

4 To grant permissions, select a permission type in **Type of Access**.

Or, to remove permissions, click **Remove**.

Notes

- 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.

{button ,AL("a_file_access_perm;a_spec_access_perm;a_add_perm")} Related Topics

To set special access permissions

1 In My Computer, select either the files or the directories you want.

2 On the **File** menu, click **Properties**.

3 Click the **Security** tab, and then click **Permissions**.

4 In **Name**, select a user or group.

5 In **Type of Access**, click one of the following:

- If you selected files in step 1, click **Special Access**.
- If you selected directories in step 1 and want to set permissions on all the files in them, click **Special File Access**.
- If you selected directories in step 1 and want to set permissions on the directories but not the files in them, click **Special Directory Access**.

A **Special Access** dialog box appears.

6 Click to select or clear check boxes for the permissions you want to grant.

Or, click **Full Control (All)**, to grant all of the special access permissions.

Notes and Tips

- You can prevent files from inheriting the permissions you set for their directories. To do this, click **Special File Access** in step 5 of the procedure above, and then click **Access Not Specified** in the **Special File Access** dialog box.
- If no groups or users appear in **Name**, the directories or files you selected have different permissions. You must add a group or user before setting special access permissions.

{button ,AL("a_spec_dir_perms;a_spec_file_perms")} Related Topics

To search for a user or group account

1. In the **Add Users and Groups** dialog box, click **Search**.
2. Type the group or user name in **Find User or Group**.
3. If necessary, click **Search Only In**, and select one or more domains.
4. Click **Search**.

Tip

If you want to add accounts found in **Search Results** to the **Add Users and Groups** dialog box, select those accounts and click **Add**.