Chapter 9 Managing Files

Overview

This chapter describes:

- Types of file windows
- Types of history windows
- How to sort and filter file windows
- How to add, change, and delete file rules
- Common applications of files rules

Contents

Viewing Directories and Files

File Manager displays directory and file information for the current resource based on the File History Database and the resource's disk. Files that are currently on disk are represented by yellow document icons. Files that have been deleted from disk but have file history recorded are represented by gray document icons. Gray folder icons represent deleted directories.

> **NOTE:** In 4.x installations, any user who needs access to File Manager must be logged in to the tree where Backup Director is installed.

The drive bar displays all of the resources and/or drives that you are currently mapped or connected to.

File Manager Tool Bar

The File Manager tool bar provides a short cut to commonly used operations:

Define Filter–Specify the filename pattern and/or other criteria.

Enable Filter–Apply the defined filter and display only those files that match the filename pattern and/or criteria during the session.

Sort–Sort files by specified criteria.

File Finder–Find files that match the specified criteria.

Backup–Back up tagged directories and/or files.

Restore–Restore the selected item(s).

Help–Open the Help menu.

Viewing the File Window

To view directories and files

1. To view a resource that you are currently mapped to or connected to, select the corresponding button from the drive bar. Tool Tips identify a workstation drive or other network resource.

or

1. To specify a resource that you are not currently mapped to, open the File menu and select the *Open Resource* option. The Open Resource dialog box appears. Choose the **Resource** button to display the installation's protected installation.

   > **NOTE:** End users do not have the *Open Resource* menu option. The drive bar displays resources that the end users are mapped to. By selecting a drive icon, end users can view the directories and files for which they have read rights residing on the selected resource.

   > \> If you are selecting a resource on another installations, you must first select an installation and then choose the **Resources** button.

2. In the **Installation Resources** list box, click the resource.

3. Choose **OK**. The directory and file windows appear.

> If the program cannot find the physical resource you selected, a prompt informs you that the resource is off-line. You can continue with the operation and view the database records for the resource; you cannot view files on the disk. You can also view the specific system message.

The file window lists the files residing in the highlighted directory. The *View* menu lists three options that provide different information about the files currently listed:

- File Attributes
- File Path
- File Rules

To view a different file window display

> Open the View menu and choose *File Attributes*, *File Path*, or *File Rules*.

Viewing File Attributes

File Attributes, the default display of the file window, includes the file attribute, Create/Modify date, and size information. Because Backup Director does not know the level of security defined for a deleted directory, it cannot display any deleted directories to end users. A file may have one or more of the following attributes:

Attribute	**Indicates**
a	The archive bit has been set for this file on disk.
r	This file is read only.
h	This file is a hidden file.
s	This file is a system file.

Viewing File Path

The *File Path* option displays the directory path in which a file is located. This view can be useful to list files that have similar name patterns or tagged files from different directories.

Viewing File Rules

The *File Rules* option displays the file rules that apply to files in the highlighted directory or root. To access menu options under the Rules menu, you must be viewing the File Rules window.

Updating the File Window

If you or another user performs an operation on a file while you are in File Manager, you will not see the effect of the operation (such as a restore) unless you select Operations/*Refresh Directory Tree*.

Viewing the File Versions

File History Window

The File History window displays all of the versions of the highlighted file that exist on backup media. Each file version displays the Create/Modify date and byte size.

Extended History Window

The Extended History window displays the number of backup copies on media for a specific file. The Extended History window also has a **Restore** button to restore a selected version on a specific session.

To view the media location of a file version

1. Highlight a file version in the File History window.

2. Open the View menu and select *Extended History*. The Extended History window appears.

Parameter	**Description**
File	The selected filename.
Path	The directory path of the selected file version.
Media	The label of the media containing a copy of the selected file version.
Session	The session number that contains the selected file version.
Size	The size of the file version as written to the session. “CP” indicates a backup session.
Create/Modify	The time and date the file version was last modified.

Tagging Files and Directories

Tagging indicates which directories and files have been selected for an operation. See chapter 3 for instructions on how to tag and untag items.

To tag a file or directory

> Click the check box to the left of the filename or directory. The red “x” next to the filename indicates that the file is tagged for an operation. The gray “x” in the directory check box indicates that one or more files in a collapsed subdirectory are tagged.

To view the next tagged item

> From either the directory or file window, open the Select menu and choose *Next Tagged Item*. The cursor moves to the next tagged item in that window. In the directory window, the cursor also moves to the next directory on which only some of the files have been tagged.

Before you perform an operation on tagged files, you may want to review the files that will be included in the operation. This can be difficult if the files are located in many directories.

To view all tagged files

> After tagging files, open the View menu and select *Tagged Items Window*.

Changing Directories

To view specific directories on the current resource

1. Open the Tree menu and choose *Change Directory*. The Path Selection dialog box appears.

2. Type the path that you want to view. For example, to move from the root of the SYS: volume to SYS:\SYSTEM, type **SYSTEM** in the dialog box.

3. To move to a directory on the same level, type the entire path or the relative path. For example, to move from SYS:\SYSTEM to SYS:\LOGIN, you must type **\LOGIN** or **..\LOGIN** in the dialog box.

4. After typing in the path, choose **OK**.

Removing History Records

Directories that have been deleted from disk are represented by gray folder icons. The File History Database maintains these records so that you can restore these directories. If you no longer want to be able to restore these directories, you can remove these records. Removing the records does **not** reduce the size of the database or make additional space available on the disk.

WARNING: Remove history records from the database only if you are certain that you will not need to restore these directories.

To remove a directory's history records

1. Tag the deleted directory. The deleted directory has a gray folder icon.

2. Open the Operations menu and select *Remove History Record*. The directory disappears from the directory tree.

NOTE: End users cannot view deleted directories.

Sorting Files

The sorting features can help you arrange files residing on a particular directory.

To sort files

> Open the View menu and select the *Sort* option. The Sort Options dialog box appears. Select the feature on which you want to sort: name, extension, date, size, attribute type, or no order. Then indicate whether you want to rank the items in ascending or descending order by feature before choosing **OK**.

Filtering Files

Filtering files allows you to view only those files that are relevant to the operation you want to perform. The filter you define applies to any resource you open during the current session. This option allows you to narrow your search even if you know only a few details about the file.

Before you filter the file window, you should understand how the display is defined by default. The file window is based on records in the File History Database and those files currently on the resource's disk.

The file records can include files and directories that been deleted from the disk. So by default, a file (or directory) may be in one of three states in the file window:

- The file is on both the disk and the database.
- The file is deleted from the disk and marked for deletion from the database.
- The file is deleted from both the disk and the database. When a file is deleted from the history database, the program no longer records history for the file.

To filter files

1. Open the View menu and select the *Define Filter* menu option. The File Finder Parameters dialog box appears.

2. In the **File Name Pattern(s)** parameter, type the name of the file or part of the name and wild cards. When entering more than one pattern (you can enter up to 10 patterns), separate each with a comma (“,”) to find several different patterns during one search. For example, you can type ***.EXE,*.BAT** in the **File Name Pattern(s)** text box to find files matching those patterns.

3. Select the option combination that selects the source of the files that you want to view. For example, select the **Display Files on Disk** and the **No Deleted Files** options to view files only on the disk. Descriptions of other combinations appear in the table.

Display Files on Disk and **All Deleted Files**−Displays all files for which there are records in the File History Database and files currently on the disk. This is the default display of the file window.

Display Files on Disk and **Files Deleted as of__**−Displays files that are on disk and files deleted from disk between the present and specified number of days.

Display Files on Disk and **No Deleted Files**−Displays only the files that are on disk.

All Deleted Files−When **Display Files on Disk** is turned off, the program displays all files deleted from the disk that have also been recorded in the File History Database.

Files Deleted as of __−When **Display Files on Disk** is turned off, the program displays files that have been deleted from the disk between the present and specified number of days. This option combination is useful for identifying files deleted recently. You may be able to restore them from a backup session and preserve the continuity of the file's history if you have updated file records on the database (or the rotation has not yet occurred).

1. Select the **Advanced** button if you want to define additional criteria on which to filter the file window. The parameters are:

   Date Range−Finds file versions that have a modification date within the date range you specify. The program displays file versions that exist on the resource or on media which have a version in the specified date range.

   Start−Specify the earliest date and time for the date range you are filtering.

   End−Specify the latest date and time for the date range you are filtering.

   File Size−Search for files that are greater than, equal to, or less than the specified size (in bytes).

2. Choose **OK** to save the filter parameters.

3. Open the View menu and select *Enable Filter* to apply the filter to the window. To toggle between

a filtered and an unfiltered file window by selecting *Enable Filter*.

> **TIP:** You can use *SubTree* in conjunction with the *Enable Filter* options to tag items that match criteria you specify.
>
> After choosing your filter, move your cursor to the root directory and select *SubTree*. This will tag all of the items on the resource that match your filter criteria.

Finding Files

Use *File Finder* to quickly find files on your resource that match parameters you define.

To find a file

1. Open the Operations menu and choose *File Finder*. The File Finder Parameters dialog box appears.

2. In the **Starting Search Path** parameter, enter the directory path that you want the search to begin on the current resource. By default the currently highlighted directory appears in the **Starting Search Path** parameter of the File Finder Parameters dialog box and the program searches for any file (the wild card pattern) in that directory.

3. To search a different directory path on the current resource, type a directory name to start searching from that directory. If you type a "\" as the search path, the program searches the entire resource from the root directory.

4. In the **File Name Pattern(s)** parameter, type the name of the file or part of the name and wild cards. When entering more than one pattern (you can enter up to 10 patterns), separate each with a comma (",") to find several different patterns during one search. For example, you can type ***.EXE,*.BAT** in the **File Name Pattern(s)** text box to find files matching those patterns.

5. Choose **OK** start searching for the file. All matching files are found and displayed in a separate window with a history window. From either window you can tag and restore files.

> **TIP:** File Finder can be a useful way of doing a "WhereIs" or "NDir" operation for an item that is no longer on disk.

Customizing File Rules

The File Rules window displays the file rule in effect for files in the current directory. From any directory you view all of the rules that apply to the current resource.

- **Include**−Files with this backup rule are always available for backup operations.
- **Exclude**−Files with this backup rule never available for backup operations. This rule conserves media and reduces processing time.

To view the file rules of the current resource

> \> Once you have selected View/*File Rules*, open the *Rules* menu and select the *File Rules* option. The Rule List window displays all rules that have been created for current resource. The Palindrome logo identifies a system rule.

The File Rules window shows rules created for the current directory. If no rules have been created in the current directory, you can view the origin of a particular file's rule using Rules/*Rule Origin* or view all of the rules for the resource on the Rule List window.

To view the source of a file's rule

> Highlight the filename and select Rules/*Rule Origin*. The Rule Origin window appears.

Backup Director comes with a defined set of rules that ensures the appropriate protection of files on most LANs. Most likely you will not need to change your file rules. Some resources, however, may have files (or groups of files) that do not need protection. For example, to save time and media, you may want Backup Director to exclude unwanted files such as *.BAK files from backup operations.

System Resource Rules

Backup Director automatically assigns file-specific rules for its own databases, workstation volumes, and NetWare servers. Note that although the *.PAC file rules are set to **Exclude**, the program protects these files by writing them to their own DH and DC sessions at every full backup, incremental, or differential operation.

Because network requirements vary depending on the environment, corporate policy, government specifications, etc., you may find it necessary to customize system rules to meet your requirements.

Other Backup Director System Rules

Resources with File History Database

\PAL (Installation Directory)

AS??.PAC, Exclude
ST??.PAC, Exclude
AV*.PAC, Exclude
TMP*, Exclude
COMMANDS, Exclude

Resources with System Control Database

\PNA (Installation Directory)

*.HLP, Exclude

*.EXE, Include

*.RSF, Exclude

AS*.PAC, Exclude

TMPDB*, Exclude

DOS Workstation Volumes

\CONFIG.SYS, Include

\COMMAND.COM, Include

\AUTOEXEC.BAT, Include

*.SYS, Include

\IBM*.COM, Include

OS/2 Workstation Volumes

\CONFIG.SYS, Include

\EA DATA. SF, Exclude

\WP ROOT. SF, Include

\STARTUP.CMD, Include

\OS2LDR, Include

\OS2LDR.MSG, Include

\OS2KRNL, Include

\OS2BOOT, Include

\NET.CFG, Include

\SWAPPER.DAT, Exclude

\OS2

CMD.EXE, Include

*.INI, Include

Rules for NetWare Volumes

*.Q, Exclude

\Trash Can Usage Map, Exclude

Q_*, Exclude

Q$*, Exclude

\DIRSTAMP.SYS, Exclude

SYS:

\BACKOUT.TTS, Exclude

\SYSTEM

*, Include

SYS$LOG.ERR, Include

TSA*.DER, Exclude

\PUBLIC

*, Include

\LOGIN

*, Include

\MAIL

*, Include

How Rules Affect Resources, Directories, and Files

Rules may be defined for an entire resource (although not for an entire server), a directory, a group of files, or an individual file. By default, when you create a rule, all files that match a filename pattern in the current directory are affected. The filename pattern can include wild card characters or a specific filename.

- A rule is more specific if it occurs farther down in a directory tree.
- A rule is more specific if it is defined with a more restrictive (less generic) filename pattern.

Any rule in a subdirectory takes precedence over rules in the directories above. If two rules are defined in the same directory, the more specific one takes precedence for the files it covers.

For example, “*” is the least specific filename pattern, and an individual filename (ABC.WK1) is the most specific pattern.

The following list of filename patterns is arranged from least specific to most specific.

* (Least specific)
.W
*.WK?
*.WK1
A*.WK1
ABC.WK1 (Most specific)

If rules were defined for all six filename patterns in a single directory in the above example:

- The ABC.WK1 rules would be the effective rules for the file ABC.WK1.
- Any WK1 file that started with an A (except ABC.WK1) would be covered by the A*.WK1 rules. All other WK1 files would be covered by the *.WK1 rules.
- Any files with an extension of WKS would be covered by the *.WK? rules. The *.W* rules would cover any files that have an extension beginning with “W,” unless they were covered by a more specific pattern.
- All other files would be covered by the * rules.

Enhancing the Effect of a Rule

By default, the program applies a new rule only to matching files within the current directory. You can determine whether the program will apply the file rule to like-named files in subdirectories. The **Apply to Subtree** option allows you to control the impact of a rule. You can turn on the **Apply to Subtree** option and apply the new rule to matching files along the subtree. For example, if you select this option when creating a rule for the filename pattern "*.WK*" at the root of the resource (the "\" directory), all files on the entire resource matching that pattern are affected.

The procedure for adding file-specific rules is detailed below in the "*Adding Rules*" section.

> **NOTE:** To be protected, all files must be governed by a rule. To ensure that all files on your protected resources are covered by a file rule, you cannot turn off the **Apply to Subtree** option for any system rule. System rules are identified by the Palindrome logo on the Rule List window.

Changing, Adding, and Deleting Rules

This section describes how to change, add and delete rules to customize Backup Director to your environment. Rules allow you to refine your operations by excluding or including certain kinds of files from backup operations. You can add, delete, and edit file rules.

Changing Rules

To change a rule

1. From the File Rule window, highlight the rule you want to edit. Rules for a filename pattern defined for the current directory appear at the top of the File Rules window. File-specific icons appear next to the filename.

2. Open the Rules menu and select *Edit Rule*. The Rule Definition dialog box appears with the backup rules applicable to the currently highlighted file rule.

3. By default, the changes to the updated rule apply only to matching files in the current directory. To apply the updated file rule to a matching filenames throughout the subtree, select the **Apply to Subtree** option.

4. Choose **OK** to save the changes. The File Rules window displays the result of your change.

Adding Rules

Most of your changes to file rules will be due to adding more specific rules to supersede system rules. For example, add a rule in the root directory for *.BAK or other extensions, and set the rules to **Backup/Include**. This prevents BAK files from being backed up. As a result, backup operations require less time and media.

To add a rule

1. Select the resource on which you want to create a rule.

2. With your cursor at the appropriate directory, open the *View* menu and choose *File Rules*. The File Rules window appears.

3. From the File Rules window, highlight any item whose rule you want to make more specific.

4. Open the Rule menu and select *Insert Rule*. The Rules Definition dialog box appears.

5. In the **File Pattern** parameter, type the file pattern (or specific file) that you want to add a rule for.

For example, to add a rule for all files in the directory with the file pattern *.BAK, type ***.BAK**.

6. Indicate whether this rule will become effective for subdirectory files.

   > To apply this rule to subdirectory files, select **Apply to Subtree**.

7. Choose **OK**. The new rule appears in the file window.

Deleting Rules

You can delete a rule for a specific filename pattern using the steps below.

> **NOTE:** You cannot delete system rules or edit the **Apply to Subtree** option of system rules. If there are no specific file pattern rules, every file is automatically covered by a set of system rules.

To delete a rule

1. With your cursor at the root of the appropriate directory, open the *View* menu and choose *File Rules*. The File Rules window appears.

2. Highlight the rule you want to delete.

3. Open the Rules menu select *Delete Rule*. The Rule Definition dialog box appears.

4. Confirm that this is the rule you want to delete and choose **OK**. The rule no longer appears on the Rules List window. Another rule with a less specific filename pattern or path replaces the deleted rule.

End User File Manager

The end user version of File Manager provides the essential backup and restore operations. To perform operations, end users must have access to File Manager (PALFILER.EXE) and be given rights to the File History Databases of their files.

To give end users access to File Manager

1. During installation, File Manager is copied to the installation directory. You can allow users to access the installation directory or copy PALFILER.EXE to one or more public directories.

   > If you copy PALFILER.EXE to a public directory, be sure to also copy the resource (*.RSF), help (*.HLP), and *.DLL files from the installation directory to the public directory.

2. Grant users Read and File Scan rights to the Backup Director installation directory (or public directory) so they can access PALFILER.EXE.

   > If you have distributed File History Databases, grant rights to the installation directory of each of those servers.

   > If you have a group EVERYONE, grant that group Read and File Scan rights to the same directories.

   > If you have multiple installations or PALFILER.EXE exists on servers other than

your installation server, create a File Manager rights user with Read and File Scan rights to the installation directory. The File Manager rights user allows end users who are not attached to the installation server to access the File History Database. You will specify this user later (“*Configuring Access to an Installation*” section).

To create the File Manager icon

1. From the Windows desktop of each end user's workstation, open the File menu and select *New*. Create the program group.

2. Open the File menu and select *New*. Create a new program item.

3. Type **File Manager** in the **Description** parameter.

4. Use the **Browse** button to complete the command line. Select the public directory path and PALFILER.EXE.

5. Choose **OK** to confirm the properties. At the Network Path Specified prompt, choose **Yes** to continue .

Configuring Access to an Installation

If you copy PALFILER.EXE to a public directory or if you have multiple installations, you must configure the Backup Director installation(s) that users can access when using File Manager.

If you have multiple copies of PALFILER.EXE

1. Access File Manager.

2. Open the File menu and select *Enterprise Setup*. The Installation Configuration dialog box appears.

3. Choose **Insert**.

4. From the Select Installation dialog box, select the installation you want end users to have access to and choose **OK**.

5. Choose the **User** button to configure the name and password of the File Manager rights user. This is the user that you created above (“To give end users access to File Manager” steps).

6. Choose **OK**.

7. Choose **Close** to exit.

Only administrators (defined on the Admin List in Configuration Manager) can configure rules, add installations, etc. within File Manager. Whenever users access a resource (using the drive bar or the File/*Open Resource* option), they will be prompted for a login name and password. While users access the Installation Configuration dialog box, they cannot make any changes since they do not have the appropriate NetWare rights to the installation.

To submit jobs, end users must be defined in the User List in Configuration Manager or the jobs will fail. The group EVERYONE is actually added to the User List during the install.

Configuring End User Workstations

If you are protecting workstations and you want end users to be able to submit backup and restore jobs for their workstation files, each workstation must be configured. Although end users' local drives are on the Protected Resource List, they cannot access database records for their own workstations by default. Use the Preferences option to allow end users to view the files and database records of their local drive.

To configure an end user's protected workstation

1. In File Manager, open the File menu and select *Preferences*.

2. Specify the workstation name as it appears in the Protected Resource List.

   > To configure workstation names using an environment variable in a system login script, select **Environment**. This is the default selection. Use “WSNAME” (or a another name you specify) in the login script to configure workstations automatically.

   > If you are not using an environment variable for the names of the protected workstations, select **Specific**. You must type the workstation name as it appears in the Protected Resource List. With this option you must configure the name at each workstation.

3. Choose **OK**.

Notification

End users configure notification through *Preferences*. Backup Director can notify end users about the status of restore requests. Each user can choose how they want to be notified prior to submitting the request.

To receive notification through e-mail

1. Open the File menu and select *Preferences*. The Preferences dialog box appears. File Manager's Preferences dialog box is similar to those of the other managers. The drive bar is an additional option.

2. Specify the notification you want to receive. You can specify one or both types.

   > Select **Novell Send**. This operation notifies end users if a restore job failed or succeeded.

   > Select **E-Mail**. Choose a method for specifying e-mail addresses:

   Specific–Select this option to specify the e-mail address for each individual workstation. Enter your e-mail account name and address in the **E-mail Address** text box. The correct format is “USER@WORKGROUP” (for example, “JSMITH@PALINDRO”).

   Environment–Select this option to automatically use an e-mail environment variable to configure all e-mail reports. Use “FMUSER” (or another name you specify).

3. Choose **OK** to save the notification parameters.